

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/002514

International filing date: 10 February 2005 (10.02.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-169001
Filing date: 07 June 2004 (07.06.2004)

Date of receipt at the International Bureau: 31 March 2005 (31.03.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

10. 2. 2005

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 4 年 6 月 7 日
Date of Application:

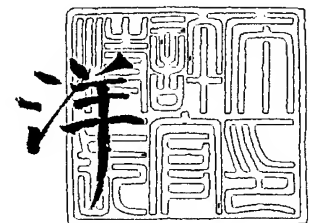
出 願 番 号 特 願 2 0 0 4 - 1 6 9 0 0 1
Application Number:
[ST. 10/C]: [J P 2 0 0 4 - 1 6 9 0 0 1]

出 願 人 エヌ・ティ・ティ・コミュニケーションズ株式会社
Applicant(s):

2 0 0 5 年 3 月 1 8 日

特許庁長官
Commissioner,
Japan Patent Office

小 川



【書類名】 特許願
【整理番号】 GLN-00497
【提出日】 平成16年 6月 7日
【あて先】 特許庁長官殿
【国際特許分類】 G09C 1/00
【発明者】
 【住所又は居所】 東京都千代田区内幸町一丁目 1 番 6 号 エヌ・ティ・ティ・コ
 ミュニケーションズ株式会社内
 【氏名】 荻原 利彦
【発明者】
 【住所又は居所】 東京都千代田区内幸町一丁目 1 番 6 号 エヌ・ティ・ティ・コ
 ミュニケーションズ株式会社内
 【氏名】 加賀谷 誠
【発明者】
 【住所又は居所】 東京都千代田区内幸町一丁目 1 番 6 号 エヌ・ティ・ティ・コ
 ミュニケーションズ株式会社内
 【氏名】 野村 進
【特許出願人】
 【識別番号】 399035766
 【氏名又は名称】 エヌ・ティ・ティ・コミュニケーションズ株式会社
【代理人】
 【識別番号】 100083806
 【弁理士】
 【氏名又は名称】 三好 秀和
 【電話番号】 03-3504-3075
【選任した代理人】
 【識別番号】 100068342
 【弁理士】
 【氏名又は名称】 三好 保男
【選任した代理人】
 【識別番号】 100095500
 【弁理士】
 【氏名又は名称】 伊藤 正和
【選任した代理人】
 【識別番号】 100101247
 【弁理士】
 【氏名又は名称】 高橋 俊一
【選任した代理人】
 【識別番号】 100098327
 【弁理士】
 【氏名又は名称】 高松 俊雄
【手数料の表示】
 【予納台帳番号】 001982
 【納付金額】 16,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9908855

【書類名】 特許請求の範囲**【請求項 1】**

データをバーナム暗号を用いて暗号化する端末を複数備えており、該端末間における前記データのアクセス権限譲渡を管理するアクセス権管理システムであって、

前記データのアクセス権限を有する譲渡側端末において、該譲渡側端末の第 1 の暗号鍵で前記データを暗号化し、第 1 の暗号データを生成する手段と、

前記第 1 の暗号データを前記譲渡側端末から、前記データのアクセス権限を譲り受ける譲受側端末に送信する手段と、

前記譲受側端末において、前記譲受側端末の第 2 の暗号鍵で前記第 1 の暗号データを暗号化し、第 2 の暗号データを生成する手段と、

前記第 2 の暗号データを前記譲受側端末から前記譲渡側端末に送信する手段と、

前記譲渡側端末において、前記譲渡側端末の前記第 1 の暗号鍵で前記第 2 の暗号データを暗号化し、第 3 の暗号データを生成する手段と、

前記第 3 の暗号データを前記譲渡側端末から前記譲受側端末に送信する手段と、

前記譲受側端末において、前記第 3 の暗号データを、アクセス権限を譲り受けたデータとして所定の記憶部に記憶する手段と、

を有することを特徴とするアクセス権管理システム。

【請求項 2】

前記譲受側端末において、前記記憶部に記憶された前記第 3 の暗号データを前記第 2 の暗号鍵で復号し、前記データを生成する手段を有することを特徴とする請求項 1 記載のアクセス権管理システム。

【請求項 3】

複数の端末と相互に通信可能であり、バーナム暗号を用いて該端末間におけるデータのアクセス権限譲渡を管理するアクセス権管理装置であって、

前記データのアクセス権限を有する譲渡側端末の第 1 の暗号鍵を生成し、該第 1 の暗号鍵で前記データを暗号化し、第 1 の暗号データを生成する手段と、

前記第 1 の暗号データを所定の記憶部に前記譲渡側端末がアクセス権限を有するデータとして記憶する手段と、

前記第 1 の暗号鍵を前記譲渡側端末に送信する手段と、

前記データのアクセス権限を譲渡するときは、前記譲渡側端末から前記第 1 の暗号鍵を受信する手段と、

前記データのアクセス権限を譲り受ける譲受側端末の第 2 の暗号鍵を生成し、前記記憶部に記憶された第 1 の暗号データを、受信した第 1 の暗号鍵及び生成した第 2 の暗号鍵で暗号化し、第 2 の暗号データを生成する手段と、

前記第 2 の暗号データを前記記憶部に前記譲受側端末がアクセス権限を有するデータとして記憶する手段と、

前記第 2 の暗号鍵を前記譲渡側端末に送信する手段と、

を有することを特徴とするアクセス権管理装置。

【請求項 4】

前記データが使用されるときは、前記譲受側端末から前記第 2 の暗号鍵を受信する手段と、

前記記憶部に記憶された第 2 の暗号データを、受信した第 2 の暗号鍵で復号化し、前記データを生成する手段と、

を有することを特徴とする請求項 3 記載のアクセス権管理装置。

【請求項 5】

複数の端末と相互に通信可能であり、秘密分散法を用いて該端末間におけるデータのアクセス権限譲渡を管理するアクセス権管理装置であって、

前記秘密分散法は、

前記データを所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、前記データを処理単位ビット長毎に区分けして、複数の元部分デ

ータを生成し、この複数の元部分データの各々に対応して、前記データのビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、

新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、前記各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、前記所望の分割数の再分割データを生成するデータ分割方法であり、

前記データのアクセス権限を有する譲渡側端末の第1の乱数を生成し、該第1の乱数及び前記データから前記秘密分散法を用いて、複数の分割データを生成する手段と、

前記複数の分割データの一部を、前記譲渡側端末に送信する手段と、

前記複数の分割データの残りを、所定の記憶部に前記譲渡側端末がアクセス権限を有するデータとして記憶する手段と、

前記データのアクセス権限を譲渡するときは、前記譲渡側端末から前記分割データの一部を受信する手段と、

前記データのアクセス権限を譲り受ける譲受側端末の第2の乱数を生成し、該第2の乱数、並びに受信した分割データの一部及び前記記憶部に記憶された分割データの残りのうち前記秘密分散法を用いて、複数の再分割データを生成する手段と、

前記複数の再分割データの一部を、前記譲受側端末に送信する手段と、

前記複数の再分割データの残りを、前記記憶部に前記譲受側端末がアクセス権限を有するデータとして記憶する手段と、

を有することを特徴とするアクセス権管理装置。

【請求項6】

前記データが使用されるときは、前記譲受側端末から前記再分割データの一部を受信する手段と、

受信した再分割データの一部、及び前記記憶部に記憶された再分割データの残りのうち、復元可能な所定の個数の再分割データの組み合わせから前記秘密分散法を用いて前記データを復元する手段と、

を有することを特徴とする請求項5記載のアクセス権管理装置。

【請求項7】

前記秘密分散法は、前記各分割部分データの定義式における乱数部分データを、該乱数部分データに対応する新たな乱数部分データに置換した各再分割部分データの定義式により、各再分割部分データを生成することを特徴とする請求項5又は6記載のアクセス権管理装置。

【請求項8】

データをバーナム暗号を用いて暗号化する端末を複数備えたアクセス権管理システムの該端末間における前記データのアクセス権限譲渡を管理するアクセス権管理方法であって、

前記データのアクセス権限を有する譲渡側端末において、該譲渡側端末の第1の暗号鍵で前記データを暗号化し、第1の暗号データを生成するステップと、

前記第1の暗号データを前記譲渡側端末から、前記データのアクセス権限を譲り受ける譲受側端末に送信するステップと、

前記譲受側端末において、前記譲受側端末の第2の暗号鍵で前記第1の暗号データを暗号化し、第2の暗号データを生成するステップと、

前記第2の暗号データを前記譲受側端末から前記譲渡側端末に送信するステップと、

前記譲渡側端末において、前記譲渡側端末の前記第1の暗号鍵で前記第2の暗号データを暗号化し、第3の暗号データを生成するステップと、

前記第3の暗号データを前記譲渡側端末から前記譲受側端末に送信するステップと、

前記譲受側端末において、前記第3の暗号データを、アクセス権限を譲り受けたデータ

として所定の記憶部に記憶するステップと、
を有することを特徴とするアクセス権管理方法。

【請求項 9】

複数の端末と相互に通信可能なアクセス権管理装置が、バーナム暗号を用いて該端末間におけるデータのアクセス権限譲渡を管理するアクセス権管理方法であって、

前記データのアクセス権限を有する譲渡側端末の第 1 の暗号鍵を生成し、該第 1 の暗号鍵で前記データを暗号化し、第 1 の暗号データを生成するステップと、

前記第 1 の暗号データを所定の記憶部に前記譲渡側端末がアクセス権限を有するデータとして記憶するステップと、

前記第 1 の暗号鍵を前記譲渡側端末に送信するステップと、

前記データのアクセス権限を譲渡するときは、前記譲渡側端末から前記第 1 の暗号鍵を受信するステップと、

前記データのアクセス権限を譲り受ける譲受側端末の第 2 の暗号鍵を生成し、前記記憶部に記憶された第 1 の暗号データを、受信した第 1 の暗号鍵及び生成した第 2 の暗号鍵で暗号化し、第 2 の暗号データを生成するステップと、

前記第 2 の暗号データを所定の記憶部に前記譲受側端末がアクセス権限を有するデータとして記憶するステップと、

前記第 2 の暗号鍵を前記譲渡側端末に送信するステップと、

を有することを特徴とするアクセス権管理方法。

【請求項 10】

複数の端末と相互に通信可能なアクセス権管理装置が、秘密分散法を用いて該端末間におけるデータのアクセス権限譲渡を管理するアクセス権管理方法であって、

前記秘密分散法は、

前記データを所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、前記データを処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、前記データのビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、

新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、前記各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、前記所望の分割数の再分割データを生成するデータ分割方法であり、

前記データのアクセス権限を有する譲渡側端末の第 1 の乱数を生成し、該第 1 の乱数及び前記データから前記秘密分散法を用いて、複数の分割データを生成するステップと、

前記複数の分割データの一部を、前記譲渡側端末に送信するステップと、

前記複数の分割データの残りを、所定の記憶部に前記譲渡側端末がアクセス権限を有するデータとして記憶するステップと、

前記データのアクセス権限を譲渡するときは、前記譲渡側端末から前記分割データの一部を受信するステップと、

前記データのアクセス権限を譲り受ける譲受側端末の第 2 の乱数を生成し、該第 2 の乱数、並びに受信した分割データの一部及び前記記憶部に記憶された分割データの残りに前記秘密分散法を用いて、複数の再分割データを生成するステップと、

前記複数の再分割データの一部を、前記譲受側端末に送信するステップと、

前記複数の再分割データの残りを、前記記憶部に前記譲受側端末がアクセス権限を有するデータとして記憶するステップと、

を有することを特徴とするアクセス権管理方法。

【請求項 11】

データをバーナム暗号を用いて暗号化する端末を複数備えており、該端末間における前

記データのアクセス権限譲渡を管理するアクセス権管理システムの端末用プログラムであって、

前記データのアクセス権限を有する譲渡側端末に、

該譲渡側端末の第1の暗号鍵で前記データを暗号化し、第1の暗号データを生成するステップと、

前記第1の暗号データを前記データのアクセス権限を譲り受ける譲受側端末に送信するステップと、

前記譲受側端末から、前記譲受側端末の第2の暗号鍵で暗号化して、生成された第2の暗号データを受信するステップと、

前記第1の暗号鍵で前記第2の暗号データを暗号し、第3の暗号データを生成するステップと、

前記第3の暗号データを、アクセス権譲渡のデータとして前記譲受側端末に送信するステップと、

を実行させることを特徴とする端末用プログラム。

【請求項12】

データをバーナム暗号を用いて暗号化する端末を複数備えており、該端末間における前記データのアクセス権限譲渡を管理するアクセス権管理システムの端末用プログラムであって、

前記データのアクセス権限を譲り受ける譲受側端末に、

前記データのアクセス権限を有する譲渡側端末から、該譲渡側端末の第1の暗号鍵で前記データを暗号化して、生成された第1の暗号データを受信するステップと、

前記譲受側端末の第2の暗号鍵で前記第1の暗号データを暗号化し、第2の暗号データを生成するステップと、

前記第2の暗号データを前記譲渡側端末に送信するステップと、

前記譲渡側端末から、前記第1の暗号鍵で前記第2の暗号データを暗号化して、生成された第3の暗号データを受信するステップと、

前記第3の暗号データを、アクセス権限を譲り受けたデータとして所定の記憶部に記憶するステップと、

を実行させることを特徴とする端末用プログラム。

【請求項13】

前記記憶部に記憶された前記第3の暗号データを前記第2の暗号鍵で復号し、前記データを生成するステップを前記譲受側端末に実行させることを特徴とする請求項12記載の端末用プログラム。

【請求項14】

複数の端末と相互に通信可能であり、バーナム暗号を用いて該端末間におけるデータのアクセス権限譲渡を管理するためのコンピュータが読み取り可能なアクセス権管理プログラムであって、

前記データのアクセス権限を有する譲渡側端末の第1の暗号鍵を生成し、該第1の暗号鍵で前記データを暗号化し、第1の暗号データを生成するステップと、

前記第1の暗号データを所定の記憶部に前記譲渡側端末がアクセス権限を有するデータとして記憶するステップと、

前記第1の暗号鍵を前記譲渡側端末に送信するステップと、

前記データのアクセス権限を譲渡するときは、前記譲渡側端末から前記第1の暗号鍵を受信するステップと、

前記データのアクセス権限を譲り受ける譲受側端末の第2の暗号鍵を生成し、前記記憶部に記憶された第1の暗号データを、受信した第1の暗号鍵及び生成した第2の暗号鍵で暗号化し、第2の暗号データを生成するステップと、

前記第2の暗号データを所定の記憶部に前記譲受側端末がアクセス権限を有するデータとして記憶するステップと、

前記第2の暗号鍵を前記譲渡側端末に送信するステップと、

を前記コンピュータに実行させることを特徴とするアクセス権管理プログラム。

【請求項 15】

前記データが使用されるときは、前記譲受側端末から前記第2の暗号鍵を受信するステップと、

前記記憶部に記憶された第2の暗号データを、受信した第2の暗号鍵で復号化し、前記データを生成するステップと、

を前記コンピュータに実行させることを特徴とする請求項14記載のアクセス権管理プログラム。

【請求項 16】

複数の端末と相互に通信可能であり、秘密分散法を用いて該端末間におけるデータのアクセス権限譲渡を管理するためのコンピュータが読み取り可能なアクセス権管理プログラムであって、

前記秘密分散法は、

前記データを所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、前記データを処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、前記データのビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、

新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、前記各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、前記所望の分割数の再分割データを生成するデータ分割方法であり、

前記データのアクセス権限を有する譲渡側端末の第1の乱数を生成し、該第1の乱数及び前記データから前記秘密分散法を用いて、複数の分割データを生成するステップと、

前記複数の分割データの一部を、前記譲渡側端末に送信するステップと、

前記複数の分割データの残りを、所定の記憶部に前記譲渡側端末がアクセス権限を有するデータとして記憶するステップと、

前記データのアクセス権限を譲渡するときは、前記譲渡側端末から前記分割データの一部を受信するステップと、

前記データのアクセス権限を譲り受ける譲受側端末の第2の乱数を生成し、該第2の乱数、並びに受信した分割データの一部及び前記記憶部に記憶された分割データの残りのうち前記秘密分散法を用いて、複数の再分割データを生成するステップと、

前記複数の再分割データの一部を、前記譲受側端末に送信するステップと、

前記複数の再分割データの残りを、前記記憶部に前記譲受側端末がアクセス権限を有するデータとして記憶するステップと、

を前記コンピュータに実行させることを特徴とするアクセス権管理プログラム。

【請求項 17】

前記データが使用されるときは、前記譲受側端末から前記再分割データの一部を受信するステップと、

受信した再分割データの一部、及び前記記憶部に記憶された再分割データの残りのうち、復元可能な所定の個数の再分割データの組み合わせから前記秘密分散法を用いて前記データを復元するステップと、

を前記コンピュータに実行させることを特徴とする請求項16記載のアクセス権管理プログラム。

【請求項 18】

前記秘密分散法は、前記各分割部分データの定義式における乱数部分データを、該乱数部分データに対応する新たな乱数部分データに置換した各再分割部分データの定義式により、各再分割部分データを生成することを特徴とする請求項16又は17記載のアクセス



権管理プログラム。

【書類名】 明細書

【発明の名称】 アクセス権管理システム、アクセス権管理装置、アクセス権管理方法、端末用プログラム、及びアクセス権管理プログラム

【技術分野】**【0001】**

本発明は、暗号化されたデータを他人に譲渡する、又は暗号化されたデータのアクセス権を他人に譲渡する場合のセキュリティ技術に関する。

【背景技術】**【0002】**

従来、自己が保有するデータへのアクセスを制限する方法の1つとして、暗号化してデータへのアクセスを制限するという方法がある。例えば、自己の秘匿したいデータ、重要な機密データなどに対して、他人からのアクセスを防ぐには、データを暗号化して保管するというものである。このような場合、暗号化されたデータは、暗号鍵の所有者以外には誰も復号できない。

【0003】

尚、この出願に関連する先行技術文献情報としては、次のものがある。

【非特許文献1】 電子商取引実証推進協議会セキュリティWG、“暗号利用技術ハンドブック（第2版）”、[Online]、[平成16年5月20日検索]、インターネット<URL: <http://www.ecom.jp/qecom/seika/naiyou/11report/ell-sec3.pdf>>

【発明の開示】**【発明が解決しようとする課題】****【0004】**

しかしながら、このような暗号化されたデータのアクセス権限を他人に譲渡したい場合（暗号化されたデータ自体を他人に譲渡したい場合も含む。以下、同じ。）には、自己の暗号鍵を他人に譲渡する場合を除けば、一旦、暗号化されたデータを自己の暗号鍵で復号化し、さらに、譲渡後、他人が自己の暗号鍵でデータを暗号化する必要がある。この場合には、暗号化されたデータが一旦、復号化され、暗号化されていない状態で譲渡されるので、この状態でデータが漏洩した場合、セキュリティが十分確保されないという問題がある。

【0005】

本発明は、上記の事情に鑑みてなされたものであり、暗号化によりアクセス制限されたデータのアクセス権限を他人に譲渡する場合であっても、データ復号化によるデータ漏洩の危険性を回避して、セキュリティを十分に確保し得るアクセス権管理システム、アクセス権管理装置、アクセス権管理方法、端末用プログラム、及びアクセス権管理プログラムを提供することを目的とする。

【課題を解決するための手段】**【0006】**

上記目的を達成するため、請求項1記載の本発明は、データをバーナム暗号を用いて暗号化する端末を複数備えており、該端末間における前記データのアクセス権限譲渡を管理するアクセス権管理システムであって、前記データのアクセス権限を有する譲渡側端末において、該譲渡側端末の第1の暗号鍵で前記データを暗号化し、第1の暗号データを生成する手段と、前記第1の暗号データを前記譲渡側端末から、前記データのアクセス権限を譲り受ける譲受側端末に送信する手段と、前記譲受側端末において、前記譲受側端末の第2の暗号鍵で前記第1の暗号データを暗号化し、第2の暗号データを生成する手段と、前記第2の暗号データを前記譲受側端末から前記譲渡側端末に送信する手段と、前記譲渡側端末において、前記譲渡側端末の前記第1の暗号鍵で前記第2の暗号データを暗号化し、第3の暗号データを生成する手段と、前記第3の暗号データを前記譲渡側端末から前記譲受側端末に送信する手段と、前記譲受側端末において、前記第3の暗号データを、アクセス権限を譲り受けたデータとして所定の記憶部に記憶する手段と、を有することを特徴とする。

【0007】

請求項2記載の本発明は、請求項1記載の発明において、前記譲受側端末において、前記記憶部に記憶された前記第3の暗号データを前記第2の暗号鍵で復号し、前記データを生成する手段を有することを特徴とする。

【0008】

請求項3記載の本発明は、複数の端末と相互に通信可能であり、バーナム暗号を用いて該端末間におけるデータのアクセス権限譲渡を管理するアクセス権管理装置であって、前記データのアクセス権限を有する譲渡側端末の第1の暗号鍵を生成し、該第1の暗号鍵で前記データを暗号化し、第1の暗号データを生成する手段と、前記第1の暗号データを所定の記憶部に前記譲渡側端末がアクセス権限を有するデータとして記憶する手段と、前記第1の暗号鍵を前記譲渡側端末に送信する手段と、前記データのアクセス権限を譲渡するときは、前記譲渡側端末から前記第1の暗号鍵を受信する手段と、前記データのアクセス権限を譲り受ける譲受側端末の第2の暗号鍵を生成し、前記記憶部に記憶された第1の暗号データを、受信した第1の暗号鍵及び生成した第2の暗号鍵で暗号化し、第2の暗号データを生成する手段と、前記第2の暗号データを前記記憶部に前記譲受側端末がアクセス権限を有するデータとして記憶する手段と、前記第2の暗号鍵を前記譲渡側端末に送信する手段と、を有することを特徴とする。

【0009】

請求項4記載の本発明は、請求項3記載の発明において、前記データが使用されるときは、前記譲受側端末から前記第2の暗号鍵を受信する手段と、前記記憶部に記憶された第2の暗号データを、受信した第2の暗号鍵で復号化し、前記データを生成する手段と、を有することを特徴とする。

【0010】

請求項5記載の本発明は、複数の端末と相互に通信可能であり、秘密分散法を用いて該端末間におけるデータのアクセス権限譲渡を管理するアクセス権管理装置であって、前記秘密分散法は、前記データを所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、前記データを処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、前記データのビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、前記各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、前記所望の分割数の再分割データを生成するデータ分割方法であり、前記データのアクセス権限を有する譲渡側端末の第1の乱数を生成し、該第1の乱数及び前記データから前記秘密分散法を用いて、複数の分割データを生成する手段と、前記複数の分割データの一部を、前記譲渡側端末に送信する手段と、前記複数の分割データの残りを、所定の記憶部に前記譲渡側端末がアクセス権限を有するデータとして記憶する手段と、前記データのアクセス権限を譲渡するときは、前記譲渡側端末から前記分割データの一部を受信する手段と、前記データのアクセス権限を譲り受ける譲受側端末の第2の乱数を生成し、該第2の乱数、並びに受信した分割データの一部及び前記記憶部に記憶された分割データの残りに前記秘密分散法を用いて、複数の再分割データを生成する手段と、前記複数の再分割データの一部を、前記譲受側端末に送信する手段と、

前記複数の再分割データの残りを、前記記憶部に前記譲受側端末がアクセス権限を有するデータとして記憶する手段と、を有することを特徴とする。

【0011】

請求項6記載の本発明は、請求項5記載の発明において、前記データが使用されるときは、前記譲受側端末から前記再分割データの一部を受信する手段と、受信した再分割データの一部、及び前記記憶部に記憶された再分割データの残りのうち、復元可能な所定の個数の再分割データの組み合わせから前記秘密分散法を用いて前記データを復元する手段と

、を有することを特徴とする。

【0012】

請求項7記載の本発明は、請求項5又は6記載の発明において、前記秘密分散法は、前記各分割部分データの定義式における乱数部分データを、該乱数部分データに対応する新たな乱数部分データに置換した各再分割部分データの定義式により、各再分割部分データを生成することを特徴とする。

【0013】

請求項8記載の本発明は、データをバーナム暗号を用いて暗号化する端末を複数備えたアクセス権管理システムの該端末間における前記データのアクセス権限譲渡を管理するアクセス権管理方法であって、前記データのアクセス権限を有する譲渡側端末において、該譲渡側端末の第1の暗号鍵で前記データを暗号化し、第1の暗号データを生成するステップと、前記第1の暗号データを前記譲渡側端末から、前記データのアクセス権限を譲り受ける譲受側端末に送信するステップと、前記譲受側端末において、前記譲受側端末の第2の暗号鍵で前記第1の暗号データを暗号化し、第2の暗号データを生成するステップと、前記第2の暗号データを前記譲受側端末から前記譲渡側端末に送信するステップと、前記譲渡側端末において、前記譲渡側端末の前記第1の暗号鍵で前記第2の暗号データを暗号化し、第3の暗号データを生成するステップと、前記第3の暗号データを前記譲渡側端末から前記譲受側端末に送信するステップと、前記譲受側端末において、前記第3の暗号データを、アクセス権限を譲り受けたデータとして所定の記憶部に記憶するステップと、を有することを特徴とする。

【0014】

請求項9記載の本発明は、複数の端末と相互に通信可能なアクセス権管理装置が、バーナム暗号を用いて該端末間におけるデータのアクセス権限譲渡を管理するアクセス権管理方法であって、前記データのアクセス権限を有する譲渡側端末の第1の暗号鍵を生成し、該第1の暗号鍵で前記データを暗号化し、第1の暗号データを生成するステップと、前記第1の暗号データを所定の記憶部に前記譲渡側端末がアクセス権限を有するデータとして記憶するステップと、前記第1の暗号鍵を前記譲渡側端末に送信するステップと、前記データのアクセス権限を譲渡するときは、前記譲渡側端末から前記第1の暗号鍵を受信するステップと、前記データのアクセス権限を譲り受ける譲受側端末の第2の暗号鍵を生成し、前記記憶部に記憶された第1の暗号データを、受信した第1の暗号鍵及び生成した第2の暗号鍵で暗号化し、第2の暗号データを生成するステップと、前記第2の暗号データを所定の記憶部に前記譲受側端末がアクセス権限を有するデータとして記憶するステップと、前記第2の暗号鍵を前記譲渡側端末に送信するステップと、を有することを特徴とする。

【0015】

請求項10記載の本発明は、複数の端末と相互に通信可能なアクセス権管理装置が、秘密分散法を用いて該端末間におけるデータのアクセス権限譲渡を管理するアクセス権管理方法であって、前記秘密分散法は、前記データを所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、前記データを処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、前記データのビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、前記各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、前記所望の分割数の再分割データを生成するデータ分割方法であり、前記データのアクセス権限を有する譲渡側端末の第1の乱数を生成し、該第1の乱数及び前記データから前記秘密分散法を用いて、複数の分割データを生成するステップと、前記複数の分割データの一部を、前記譲渡側端末に送信するステップと、前記複数の分割データの残りを、所定の記憶部に前記譲渡側端末がアク

セス権限を有するデータとして記憶するステップと、前記データのアクセス権限を譲渡するときは、前記譲渡側端末から前記分割データの一部を受信するステップと、前記データのアクセス権限を譲り受ける譲受側端末の第2の乱数を生成し、該第2の乱数、並びに受信した分割データの一部及び前記記憶部に記憶された分割データの残りに前記秘密分散法を用いて、複数の再分割データを生成するステップと、前記複数の再分割データの一部を、前記譲受側端末に送信するステップと、前記複数の再分割データの残りを、前記記憶部に前記譲受側端末がアクセス権限を有するデータとして記憶するステップと、を有することを特徴とする。

【0016】

請求項11記載の本発明は、データをバーナム暗号を用いて暗号化する端末を複数備えており、該端末間における前記データのアクセス権限譲渡を管理するアクセス権管理システムの端末用プログラムであって、前記データのアクセス権限を有する譲渡側端末に、該譲渡側端末の第1の暗号鍵で前記データを暗号化し、第1の暗号データを生成するステップと、前記第1の暗号データを前記データのアクセス権限を譲り受ける譲受側端末に送信するステップと、前記譲受側端末から、前記譲受側端末の第2の暗号鍵で暗号化して、生成された第2の暗号データを受信するステップと、前記第1の暗号鍵で前記第2の暗号データを暗号し、第3の暗号データを生成するステップと、前記第3の暗号データを、アクセス権譲渡のデータとして前記譲受側端末に送信するステップと、を実行させることを特徴とする。

【0017】

請求項12記載の本発明は、データをバーナム暗号を用いて暗号化する端末を複数備えており、該端末間における前記データのアクセス権限譲渡を管理するアクセス権管理システムの端末用プログラムであって、前記データのアクセス権限を譲り受ける譲受側端末に、前記データのアクセス権限を有する譲渡側端末から、該譲渡側端末の第1の暗号鍵で前記データを暗号化して、生成された第1の暗号データを受信するステップと、前記譲受側端末の第2の暗号鍵で前記第1の暗号データを暗号化し、第2の暗号データを生成するステップと、前記第2の暗号データを前記譲渡側端末に送信するステップと、前記譲渡側端末から、前記第1の暗号鍵で前記第2の暗号データを暗号化して、生成された第3の暗号データを受信するステップと、前記第3の暗号データを、アクセス権限を譲り受けたデータとして所定の記憶部に記憶するステップと、を実行させることを特徴とする。

【0018】

請求項13記載の本発明は、請求項12記載の発明において、前記記憶部に記憶された前記第3の暗号データを前記第2の暗号鍵で復号し、前記データを生成するステップを前記譲受側端末に実行させることを特徴とする。

【0019】

請求項14記載の本発明は、複数の端末と相互に通信可能であり、バーナム暗号を用いて該端末間におけるデータのアクセス権限譲渡を管理するためのコンピュータが読み取り可能なアクセス権管理プログラムであって、前記データのアクセス権限を有する譲渡側端末の第1の暗号鍵を生成し、該第1の暗号鍵で前記データを暗号化し、第1の暗号データを生成するステップと、前記第1の暗号データを所定の記憶部に前記譲渡側端末がアクセス権限を有するデータとして記憶するステップと、前記第1の暗号鍵を前記譲渡側端末に送信するステップと、前記データのアクセス権限を譲渡するときは、前記譲渡側端末から前記第1の暗号鍵を受信するステップと、前記データのアクセス権限を譲り受ける譲受側端末の第2の暗号鍵を生成し、前記記憶部に記憶された第1の暗号データを、受信した第1の暗号鍵及び生成した第2の暗号鍵で暗号化し、第2の暗号データを生成するステップと、前記第2の暗号データを所定の記憶部に前記譲受側端末がアクセス権限を有するデータとして記憶するステップと、前記第2の暗号鍵を前記譲渡側端末に送信するステップと、を前記コンピュータに実行させることを特徴とする。

【0020】

請求項15記載の本発明は、請求項14記載の発明において、前記データが使用される

ときは、前記譲渡側端末から前記第2の暗号鍵を受信するステップと、前記記憶部に記憶された第2の暗号データを、受信した第2の暗号鍵で復号化し、前記データを生成するステップと、を前記コンピュータに実行させることを特徴とする。

【0021】

請求項16記載の本発明は、複数の端末と相互に通信可能であり、秘密分散法を用いて該端末間におけるデータのアクセス権限譲渡を管理するためのコンピュータが読み取り可能なアクセス権管理プログラムであって、前記秘密分散法は、前記データを所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、前記データを処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、前記データのビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、前記各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、前記所望の分割数の再分割データを生成するデータ分割方法であり、前記データのアクセス権限を有する譲渡側端末の第1の乱数を生成し、該第1の乱数及び前記データから前記秘密分散法を用いて、複数の分割データを生成するステップと、前記複数の分割データの一部を、前記譲渡側端末に送信するステップと、前記複数の分割データの残りを、所定の記憶部に前記譲渡側端末がアクセス権限を有するデータとして記憶するステップと、前記データのアクセス権限を譲渡するときは、前記譲渡側端末から前記分割データの一部を受信するステップと、前記データのアクセス権限を譲り受ける譲受側端末の第2の乱数を生成し、該第2の乱数、並びに受信した分割データの一部及び前記記憶部に記憶された分割データの残りに前記秘密分散法を用いて、複数の再分割データを生成するステップと、前記複数の再分割データの一部を、前記譲受側端末に送信するステップと、前記複数の再分割データの残りを、前記記憶部に前記譲受側端末がアクセス権限を有するデータとして記憶するステップと、を前記コンピュータに実行させることを特徴とする。

【0022】

請求項17記載の本発明は、請求項16記載の発明において、前記データが使用されるときは、前記譲渡側端末から前記再分割データの一部を受信するステップと、受信した再分割データの一部、及び前記記憶部に記憶された再分割データの残りのうち、復元可能な所定の個数の再分割データの組み合わせから前記秘密分散法を用いて前記データを復元するステップと、を前記コンピュータに実行させることを特徴とする。

【0023】

請求項18記載の本発明は、請求項16又は17記載の発明において、前記秘密分散法は、前記各分割部分データの定義式における乱数部分データを、該乱数部分データに対応する新たな乱数部分データに置換した各再分割部分データの定義式により、各再分割部分データを生成することを特徴とする。

【発明の効果】

【0024】

本発明によれば、バーナム暗号を用いて暗号化する端末を複数備え、データのアクセス権限を譲渡する譲渡側端末において第1の暗号鍵で暗号化した第1の暗号データを譲受側端末において第2の暗号鍵で暗号化して第2の暗号データとし、さらに、譲渡側端末において第2の暗号データを第1の暗号鍵で暗号化した第3の暗号データを生成し、該第3の暗号データを譲受側端末に譲渡するので、暗号化によりアクセス制限されたデータのアクセス権限を他人に譲渡する場合であっても、一旦復号せずにデータ権限を譲渡でき、セキュリティを十分に確保することができる。

【0025】

また、本発明によれば、バーナム暗号を用いて暗号化するアクセス権管理装置及び複数の端末を備え、アクセス権管理装置は、譲渡側端末のための第1の暗号鍵でデータを暗号

化して、第1の暗号データを管理し、第1の暗号鍵は譲渡側端末で管理する。そして、データのアクセス権限が譲渡された場合には、アクセス権管理装置は、譲渡側端末のための第1の暗号鍵及び譲受側端末のための第2の暗号鍵を用いて第1の暗号データをさらに暗号化し、第2の暗号データを管理し、第2の暗号鍵は譲受側端末で管理するので、暗号化によりアクセス制限されたデータのアクセス権限を他人に譲渡する場合であっても、一旦復号せずにデータ権限を譲渡でき、セキュリティを十分に確保することができる。

【0026】

また、本発明によれば、秘密分散法を用いて暗号化するアクセス権管理装置及び複数の端末を備え、アクセス権管理装置は、データを譲渡側端末の乱数を用いて秘密分散法により、分割データを生成し、該分割データの一部を譲渡側端末、残りをアクセス権管理装置で管理する。そして、譲渡側端末から譲受側端末にデータのアクセス権限が譲渡された場合には、アクセス権管理装置は、譲受側端末の新たな乱数を用いて分割データから秘密分散法により再分割データを生成し、該分割データの一部を譲受側端末、残りをアクセス権管理装置で管理するので、暗号化によりアクセス制限されたデータのアクセス権限を他人に譲渡する場合であっても、一旦復号せずにデータ権限を譲渡でき、セキュリティを十分に確保することができる。

【0027】

特に、本発明における秘密分散法は、データを所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、データを処理単位ビット長毎に区分けして、複数の元部分データを生成し、この複数の元部分データの各々に対応して、データのビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、所望の分割数の再分割データを生成するので、データを復元することなく、データを再分割することができるので、ユーザのデータをよりセキュアに管理することができる。

【発明を実施するための最良の形態】

【0028】

以下、本発明の実施の形態を図面を用いて説明する。

【0029】

<第1の実施の形態>

図1は、本発明の第1の実施の形態に係るアクセス権管理システム10の概略構成を示す図である。

【0030】

図1に示すように、アクセス権管理システム10は、ユーザが備えるクライアント端末（以下、単に端末とよぶ）1*i*（*i*=*a*, *b*）をインターネット等の通信ネットワーク2を介して接続しており、各端末1*i*が相互に通信可能となっている。尚、本実施の形態においては、1対の端末のうち、端末1*a*のユーザを甲（データ譲渡側）、端末1*b*のユーザを乙（データ譲受側）として、以下、説明する。

【0031】

各端末1*i*は、バーナム暗号を利用してデータの暗号及び復号を行う装置であり、記憶部11、データ暗号部12、データ復号部13、及び通信部14を備えている。

【0032】

ここで、バーナム暗号は、データと同じ長さの乱数列を用意し、暗号化に際してはデータの*n*ビット目と乱数列の*n*ビット目の排他的論理和演算（XOR）をし、復号化に際しては暗号化されたデータの*n*ビット目と乱数列の*n*ビット目の排他的論理和演算（XOR）をする暗号方式をいう。以下、排他的論理和演算（XOR）は、「*」なる演算記号で表すことにするが、排他的論理和演算のビット毎の演算規則での各演算結果は下記のとおりであ

る。

【0033】

0 * 0 の演算結果は 0

0 * 1 の演算結果は 1

1 * 0 の演算結果は 1

1 * 1 の演算結果は 0

また、XOR演算は交換法則、結合法則が成り立つ。すなわち、

$$a*b=b*a$$

$(a*b)*c=a*(b*c)$ が成り立つことが数学的に証明される。

【0034】

また、 $a*a=0$, $a*0=0*a=a$ が成り立つ。ここで a, b, c は同じ長さのビット列を表し、0 はこれらと同じ長さですべて「0」からなるビット列を表す。

【0035】

記憶部 11 には、ユーザがアクセスを制限したいデータ S、データ S を暗号するための暗号鍵（復号鍵）R、暗号化されたデータなどを記憶するようになっている。尚、図 1 においては、甲の暗号鍵を R、乙の暗号鍵を R' と表記して、両者を区別している。また、データ S と暗号鍵 R 及び暗号鍵 R' のデータ長は同一である。

【0036】

データ暗号部 12 は、データ S を暗号鍵 R で暗号化し、暗号データ A を生成するようになり、データ復号部 13 は、暗号データ A を暗号鍵 R で復号し、データ S を生成するようになっている。即ち、暗号化に際しては、 $A=S*R$ 、復号化に際しては、 $S=A*R$ であり、データ S と暗号鍵 R との排他的論理和演算により生成された暗号データ A を、さらに、暗号鍵 R と排他的論理和演算を行うことにより、データ S が復元されるものである。

【0037】

また、データ暗号部 12 は、後述するように、データ S を暗号化するだけでなく、他の端末 1i から送られた暗号データ A' に関しても、自己の暗号鍵 R でさらに暗号化するようになっている。また、データ復号部 13 は、後述するように、他の端末 1i から送られた暗号データ A' に関しても、自己の暗号鍵 R で復号できるようになっており、これにより、アクセス制限されたデータの譲渡が可能となっている。

【0038】

通信部 14 は、端末 1i 間における暗号データの送受信を行うようになっている。

【0039】

ここで、上述した端末 1i は、少なくとも演算機能および制御機能を備えた中央演算装置（CPU）、プログラムやデータを格納する機能を有する RAM 等からなる主記憶装置（メモリ）を有する電子的な装置から構成されているものである。また、上記装置は、主記憶装置の他、ハードディスクなどの補助記憶装置を具備していてもよい。

【0040】

このうち、データ暗号部 12、データ復号部 13、及び通信部 14 は、上記 CPU による演算制御機能を具体的に示したものに他ならない。また、記憶部 11 は、上記主記憶装置及び補助記憶装置の機能を備えたものである。

【0041】

また、本実施の形態に係る各種処理を実行するプログラムは、前述した主記憶装置またはハードディスクに格納されているものである。そして、このプログラムは、ハードディスク、フレキシブルディスク、CD-ROM、MO、DVD-ROM などのコンピュータ読み取り可能な記録媒体に記録することも、通信ネットワークを介して配信することも可能である。

【0042】

次に、本実施の形態に係るアクセス権管理システム 10 の動作を図 2 を用いて説明する。ここで、図 2 は、甲が暗号化したデータのデータ権限を乙に譲渡するときの端末 1a 及

び端末 1 b 間のデータのやりとりを示すシーケンス図である。

【0043】

まず、端末 1 a において、甲の暗号鍵 R を用いてデータ S を暗号化した暗号化データ A を生成し、記憶部 11 に保管する（ステップ S10, S20）。ここで、 $A = S * R$ である。

【0044】

次に、データ S のアクセス権限を譲渡するときは、譲渡端末 1 a から端末 1 b に暗号データ A を送信する（ステップ S30）。

【0045】

端末 1 b においては、暗号データ A を受信すると、さらに、乙の暗号鍵 R' を用いて暗号データ A を暗号化し、暗号データ A' を生成する（ステップ S40）。即ち、 $A' = A * R'$ である。

【0046】

次に、端末 1 b から端末 1 a に暗号データ A' を送信する（ステップ S50）。

【0047】

端末 1 a においては、暗号データ A' を受信すると、さらに、甲の暗号鍵 R を用いて暗号データ A' を暗号化し、暗号データ A'' を生成する（ステップ S60）。即ち、 $A'' = A' * R$ である。

【0048】

次に、端末 1 a から端末 1 b に暗号データ A'' を、アクセス権限が譲渡されたデータとして送信する（ステップ S70）。

【0049】

端末 1 b においては、受信した暗号データ A'' を記憶部 11 にアクセス権限が譲渡されたデータとして記憶する（ステップ S80）。

【0050】

次に、端末 1 b で暗号データ A'' を復号するときは、乙の暗号鍵 R' を用いて、復号されたデータ S を生成する（ステップ S90）。これは、 $A'' = A' * R$

$$= (A * R') * R$$

$$= ((S * R) * R') * R$$

$$= S * R * R' * R$$

$$= S * (R * R) * R'$$

$$= S * 0 * R'$$

$$= S * R'$$

であるから、受信した暗号データ A'' と暗号鍵 R' の排他的論理和により、

$$A'' * R' = (S * R') * R' = S$$

となることによる。尚、 $A'' = S * R'$ より、暗号データ A'' は、甲の暗号鍵 R では復号することができない。

【0051】

従って、本実施の形態に係るアクセス権管理システム 10 によれば、バーナム暗号を用いて暗号化する端末 1 a 及び 1 b を備え、データのアクセス権限を譲渡する譲渡側の端末 1 a において暗号鍵 R で暗号化した暗号データ A を譲受側の端末 1 b において暗号鍵 R' で暗号化して暗号化データ A' とし、さらに、端末 1 a において暗号化データ A' を暗号鍵 R で暗号化された暗号データ A'' を生成し、該暗号データ A'' を端末 1 b に譲渡するので、暗号化によりアクセス制限されたデータのアクセス権限を他人に譲渡する場合であっても、一旦復号せずにデータ権限を譲渡でき、セキュリティを十分に確保することができる。

【0052】

<第 2 の実施の形態>

図 3 は、本発明の第 2 の実施の形態に係るアクセス権管理システム 20 の概略構成を示

す図である。

【0053】

図3に示すように、アクセス権管理システム20は、ユーザが備えるクライアント端末（以下、単に端末とよぶ）3*i*（*i* = *a*, *b*）と、アクセス権管理サーバ4を通信ネットワーク2を介して接続しており、各端末3*i*及びアクセス権管理サーバ4が相互に通信可能となっている。尚、本実施の形態においては、1対の端末のうち、端末3*a*のユーザを甲（データ権限譲渡側）、端末3*b*のユーザを乙（データ権限譲受側）として、以下、説明する。

【0054】

各端末3*i*は、アクセスを制限したいデータ*S*を保持する端末であり、記憶部31、及び通信部32を備えている。

【0055】

記憶部31には、アクセスを制限したいデータ*S*、アクセス権管理サーバ4から送信される暗号鍵*R*（データ権限を有するユーザのデータ暗号化の際に用いられた暗号鍵）などを記憶するようになっている。尚、図1においては、甲の暗号鍵を*R*、乙の暗号鍵を*R'*と表記して、両者を区別している。また、データ*S*と暗号鍵*R*及び暗号鍵*R'*のデータ長は同一である。

【0056】

通信部32は、端末3*i*とアクセス権管理サーバ4間のデータの送受信を行うようになっている。

【0057】

アクセス権管理サーバ4は、バーナム暗号を利用してデータの暗号及び復号を行う装置であり、暗号データ記憶部41、鍵生成部42、データ暗号部43、データ復号部44、及び通信部45を備えている。

【0058】

暗号データ記憶部41は、データ暗号部43で暗号化された暗号データ*A*（データ*S*のアクセス権限を甲が有する場合の甲の暗号データ）、*A''*（データ*S*のアクセス権限を乙が有する場合の乙の暗号データ）を記憶するようになっている。

【0059】

鍵生成部42は、データ暗号部43で暗号化に用いる暗号鍵（復号鍵）*R*、*R'*を生成するようになっている。

【0060】

データ暗号部43は、端末3*a*から送信（送付）されたデータ*S*を、甲の暗号鍵*R*を用いて暗号化し、暗号データ*A*を生成するようになっている。また、データ*S*の権限を甲から乙に譲渡したときは、甲の暗号鍵*R*及び乙の暗号鍵*R'*を用いて、暗号データ*A*をさらに暗号化し、暗号化データ*A''*を生成するようになっている。尚、暗号化に用いた暗号鍵*R*及び*R'*は、それぞれ端末3*a*及び3*b*に通信部45を介して送信される。

【0061】

データ復号部44は、データ権限を譲渡されたユーザ、即ち、乙から暗号鍵*R'*が送信されると、該暗号鍵*R'*を用いて暗号化データ*A''*を復号し、データ*S*を通信部45を介して、端末3*b*に送信（送付）するようになっている。

【0062】

通信部45は、端末1*i*とアクセス権管理サーバ4間のデータの送受信を行うようになっている。

【0063】

ここで、上述した端末3*i*及びアクセス権管理サーバ4は、それぞれ、少なくとも演算機能および制御機能を備えた中央演算装置（CPU）、プログラムやデータを格納する機能を有するRAM等からなる主記憶装置（メモリ）を有する電子的な装置から構成されているものである。また、上記装置は、主記憶装置の他、ハードディスクなどの補助記憶装置を具備していてもよい。

【0064】

このうち、端末3 iの通信部3 2、アクセス権管理サーバ4の鍵生成部4 2、データ暗号部4 3、データ復号部4 4、及び通信部4 5は、上記CPUによる演算制御機能を具体的に示したものに他ならない。また、端末3 iの記憶部3 1、及びアクセス権管理サーバ4の暗号データ記憶部4 1は、上記主記憶装置及び補助記憶装置の機能を備えたものである。

【0065】

また、本実施の形態に係る各種処理を実行するプログラムは、前述した主記憶装置またはハードディスクに格納されているものである。そして、このプログラムは、ハードディスク、フレキシブルディスク、CD-ROM、MO、DVD-ROMなどのコンピュータ読み取り可能な記録媒体に記録することも、通信ネットワークを介して配信することも可能である。

【0066】

次に、本実施の形態に係るアクセス権管理システム20の動作を図4を用いて説明する。ここで、図4は、データSのデータ権限を甲から乙に譲渡するときの端末3 a、端末3 bとアクセス権管理サーバ4間のデータのやりとりを示すシーケンス図である。

【0067】

まず、甲がデータSのアクセス権限を有する場合には、データSを甲の端末3 aからアクセス管理サーバ4に送信する(ステップS110)。尚、データSの送信に際しては、通信内容の漏洩を防止するセキュアな通信ネットワーク2 a(例えば、インターネット網などのオープンな通信ネットワーク2 bではなく、LAN、IP-VPN、専用線、電話回線など)を用いる、また、通信ネットワーク2 aを介した通信ではなく、例えば、郵便などの送付手段を用いてもよい。

【0068】

アクセス権管理サーバ4は、端末3 aからデータSを受け取ると、甲の暗号鍵Rを生成し、暗号鍵Rを用いて暗号データ $A = S * R$ を生成する(ステップS120, S130)。そして、暗号データAを暗号データ記憶部4 1に記憶させるとともに、暗号鍵Rを通信ネットワーク2を介して甲の端末3 aに送信する(ステップS140, S150)。

【0069】

端末3 aは、アクセス権管理サーバ4から暗号鍵Rを受け取ると、暗号鍵Rを記憶部3 1に記憶させる(ステップS160)。

【0070】

以上の動作により、甲のデータSに対するアクセス権限は、アクセス権管理サーバ4で管理されることになる。

【0071】

次に、甲がデータSのアクセス権限を乙に譲渡する場合には、甲から乙へのデータのアクセス権譲渡の要求、及び暗号鍵Rを、甲の端末3 aから通信ネットワーク2を介してアクセス権管理サーバ4に送信する(ステップS210)。

【0072】

アクセス権管理サーバ4は、端末3 aから甲から乙へのアクセス権譲渡要求、及び暗号鍵Rを受け取ると、乙の暗号鍵R'を生成し、暗号データ記憶部4 1に記憶された暗号データAから暗号鍵R及びR'を用いて暗号データ $A'' = A * R * R'$ を生成する(ステップS220, S230)。そして、暗号データA''を暗号データ記憶部4 1に記憶させるとともに、暗号鍵R'を通信ネットワーク2を介して乙の端末3 bに送信する(ステップS240, S250)。

【0073】

端末3 bは、アクセス権管理サーバ4から暗号鍵R'を受け取ると、暗号鍵R'を記憶部3 1に記憶させる(ステップS260)。

【0074】

以上の動作により、データSに対するアクセス権限は、甲から乙に譲渡されたことにな

る。

【0075】

次に、乙がデータ S を使用する場合には、データ S の使用要求、及び暗号鍵 R' を端末 3 b から通信ネットワーク 2 を介してアクセス管理サーバ 4 に送信する（ステップ S 3 1 0）。

【0076】

アクセス権管理サーバ 4 は、端末 3 b から甲データ S の使用要求、及び暗号鍵 R' を受け取ると、暗号データ記憶部 4 1 に記憶された暗号データ A'' を暗号鍵 R' を用いて復号し、データ S を生成する（ステップ S 3 2 0）。これは、

$$\begin{aligned} A'' &= A * R * R' \\ &= (S * R) * R * R' \\ &= S * R * R * R' \\ &= S * (R * R) * R' \\ &= S * 0 * R' \\ &= S * R' \end{aligned}$$

であるから、

$$\begin{aligned} A'' * R' &= (S * R') * R' \\ &= S * R' * R' \\ &= S \end{aligned}$$

となり、データ S が得られるものである。そして、復号されたデータ S をセキュアな通信ネットワーク 2 a 又は送付手段を介して乙の端末 3 b に送信する（ステップ S 3 3 0）。

【0077】

端末 3 b は、アクセス管理サーバ 4 からデータ S を受け取ると、データ S を記憶部 3 1 に記憶させる（ステップ S 3 4 0）。これにより、乙はデータ S を端末 3 b で使用することができる。

【0078】

従って、本実施の形態に係るアクセス権管理システム 2 0 によれば、バーナム暗号を用いて暗号化するアクセス権管理サーバ 4、並びに端末 3 a 及び 3 b を備え、アクセス権管理サーバ 4 は、データのアクセス権限を譲渡する譲渡側の端末 3 a のユーザ甲のデータ S を甲の暗号鍵 R で暗号化し、暗号データ A を管理し、甲の暗号鍵は端末 3 a が管理する。そして、甲から譲受側の端末 3 b のユーザ乙にデータ S のアクセス権限が譲渡された場合には、アクセス権管理サーバ 4 は、甲の暗号鍵 R 及び乙の暗号鍵 R' を用いて暗号データ A をさらに暗号化し、暗号データ A'' を管理し、乙の暗号鍵は端末 3 b が管理するので、暗号化によりアクセス制限されたデータのアクセス権限を他人に譲渡する場合であっても、一旦復号せずにデータ権限を譲渡でき、セキュリティを十分に確保することができる。

【0079】

<第 3 の実施の形態>

（システム構成）

図 5 は、本発明の第 3 の実施の形態に係るアクセス権管理システム 3 0 の概略構成を示す図である。

【0080】

図 5 に示すように、アクセス権管理システム 3 0 は、ユーザが備えるクライアント端末（以下、単に端末とよぶ）3 i（i = a, b）と、アクセス権管理サーバ 5 を通信ネットワーク 2 を介して接続しており、各端末 3 i 及びアクセス権管理サーバ 5 が相互に通信可能となっている。また、アクセス権管理サーバ 5 は、ハードウェア的に互いに独立した複数（本実施の形態では 2 とする）のデータ保管用サーバコンピュータ（以下、単に保管サーバとよぶ）6 a, 6 b と接続されている。尚、本実施の形態においては、1 対の端末のうち、端末 3 a のユーザを甲（データ権限譲渡側）、端末 3 b のユーザを乙（データ権限譲受側）として、以下、説明する。

【0081】

各端末 3 i は、アクセスを制限したいデータ S を保持する端末であり、記憶部 3 1、及び通信部 3 2 を備えている。

【0082】

記憶部 3 1 には、アクセスを制限したいデータ S、アクセス権管理サーバ 5 から送信される分割データ D(3) などを記憶するようになっている。即ち、第 2 の実施の形態では暗号鍵 R が送信されたが、本実施の形態においては、分割データ D(3) が送信される点が異なっている。尚、図 1 においては、甲の分割データを D(3)、乙の甲の分割データを D' (3) と表記して、両者を区別している。

【0083】

通信部 3 2 は、端末 3 i とアクセス権管理サーバ 5 間のデータの送受信を行うようになっている。

【0084】

アクセス権管理サーバ 5 は、甲が権限を有するデータ S を後述する独自の秘密分散アルゴリズムによる秘密分散法（以下、秘密分散法 A とよぶ）を用いて複数のデータに分割し、該分割データを保管サーバ 6 a、6 b および端末 3 a にそれぞれ保管させるようになっている。尚、図 1 では、アクセス権管理サーバ 5 は、3 つの分割データ D(1)、D(2)、D(3) に分割し、それぞれを複数の保管サーバ 6 a、6 b および端末 3 a に保管するようになっている。

【0085】

また、アクセス権管理サーバ 5 は、データ S のデータ権限を甲から乙に譲渡する場合に、上述した秘密分散法 A を用いて、分割データ D(1)、D(2)、D(3) から再分割データ D' (1)、D' (2)、D' (3) を生成し、それぞれを複数の保管サーバ 6 a、6 b および端末 3 b に保管するようになっている。

【0086】

尚、本実施の形態においては、データ S を 3 分割して保管する場合を例に説明するが、本発明はデータ S を 3 分割する場合に限定されるわけではなく、n 分割（n = 2 以上の整数）の場合にも適用されるものである。また、端末 3 i で保管される分割データは 1 つとは限らず複数であってもよいものである。また、本実施の形態においては、分割データ D(1)、D(2)（再分割データ D' (1)、D' (2)）を保管サーバ 6、分割データ D(3)（再分割データ D' (3)）を端末 3 i に割り当てたが、どの分割データをどの保管サーバ 6 および端末 3 i に割り当ててもよいものである。さらに、本実施の形態においては、分割データ（再分割データ）の一部を保管サーバ 6 a、6 b で保管するようにしているが、アクセス権管理サーバ 5 内で管理してもよいものである。

【0087】

アクセス管理サーバ 5 は、詳しくは、データ S から複数の分割データ D を生成するために使用される乱数 R および再分割データ D' を生成するために使用される乱数 R' を発生させる乱数生成部 5 1、データ S から秘密分散法 A を用いて複数の分割データ D に分割する分割データ生成部 5 2、データ権限を甲から乙に譲渡するときに、秘密分散法 A を用いて複数の分割データ D から複数の再分割データ D' を生成する再分割データ生成部 5 3、複数の再分割データ D' から秘密分散法 A を用いてデータ S を復元するデータ復元部 5 4、並びに端末 3 i、及び保管サーバ 6 a、6 b とそれぞれデータの送受信を行う通信部 5 5 を具備する構成となっている。

【0088】

ここで、上述した端末 3 i、アクセス権管理サーバ 5 及び保管サーバ 6 a、6 b は、それぞれ、少なくとも演算機能および制御機能を備えた中央演算装置（CPU）、プログラムやデータを格納する機能を有する RAM 等からなる主記憶装置（メモリ）を有する電子的な装置から構成されているものである。また、上記装置は、主記憶装置の他、ハードディスクなどの補助記憶装置を具備していてもよい。

【0089】

このうち、端末 3 i の通信部 3 2、アクセス権管理サーバ 5 の乱数生成部 5 1、分割デ

ータ生成部52、再分割データ生成部53、データ復元部54、及び通信部55は、上記CPUによる演算制御機能を具体的に示したものに他ならない。また、端末3iの記憶部31、及び保管サーバ6a、6bは、上記主記憶装置及び補助記憶装置の機能を備えたものである。

【0090】

また、本実施の形態に係る各種処理を実行するプログラムは、前述した主記憶装置またはハードディスクに格納されているものである。そして、このプログラムは、ハードディスク、フレキシブルディスク、CD-ROM、MO、DVD-ROMなどのコンピュータ読み取り可能な記録媒体に記録することも、通信ネットワークを介して配信することも可能である。

【0091】

(秘密分散法A)

ここで、本実施の形態における独自の秘密分散アルゴリズムによる秘密分散法Aについて説明する。

【0092】

本実施形態における元データ（データSに相当する）の分割および復元では、元データを所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するが、この場合の処理単位ビット長は任意の値に設定することができ、元データを処理単位ビット長毎に区分けして、この元部分データから分割部分データを分割数より1少ない数ずつ生成するので、元データのビット長が処理単位ビット長の（分割数-1）倍の整数倍に一致しない場合は、元データの末尾の部分に0を埋めるなどして元データのビット長を処理単位ビット長の（分割数-1）倍の整数倍に合わせることで本実施形態を適用することができる。

【0093】

また、上述した乱数も（分割数-1）個の元部分データの各々に対応して処理単位ビット長のビット長を有する（分割数-1）個の乱数部分データとして乱数生成部51から生成される。すなわち、乱数は処理単位ビット長毎に区分けされて、処理単位ビット長のビット長を有する（分割数-1）個の乱数部分データとして生成される。更に、元データは処理単位ビット長に基づいて所望の分割数の分割データに分割されるが、この分割データの各々も（分割数-1）個の元部分データの各々に対応して処理単位ビット長のビット長を有する（分割数-1）個の分割部分データとして生成される。すなわち、分割データの各々は、処理単位ビット長毎に区分けされて、処理単位ビット長のビット長を有する（分割数-1）個の分割部分データとして生成される。

【0094】

なお、以下の説明では、上述した元データ、乱数、分割データ、分割数および処理単位ビット長をそれぞれS, R, D, nおよびbで表すとともに、また複数のデータや乱数などのうちの1つを表わす変数としてi(=1~n)およびj(=1~n-1)を用い、（分割数n-1）個の元部分データ、（分割数n-1）個の乱数部分データ、および分割数n個の分割データDのそれぞれのうちの1つをそれぞれS(j), R(j)およびD(i)で表記し、更に各分割データD(i)を構成する複数(n-1)の分割部分データをD(i, j)で表記するものとする。すなわち、S(j)は、元データSの先頭から処理単位ビット長毎に区分けして1番から順に採番した時のj番目の元部分データを表すものである。

【0095】

この表記を用いると、元データ、乱数データ、分割データとこれらをそれぞれ構成する元部分データ、乱数部分データ、分割部分データは、次のように表記される。

【0096】

元データS=(n-1)個の元部分データS(j)
=S(1), S(2), ..., S(n-1)

乱数R=(n-1)個の乱数部分データR(j)
=R(1), R(2), ..., R(n-1)

n個の分割データD(i)=D(1), D(2), ..., D(n)

各分割部分データ $D(i, j)$

$$\begin{aligned} &= D(1, 1), D(1, 2), \dots, D(1, n-1) \\ &\quad D(2, 1), D(2, 2), \dots, D(2, n-1) \\ &\quad \dots \quad \dots \quad \dots \\ &\quad D(n, 1), D(n, 2), \dots, D(n, n-1) \end{aligned} \quad (i=1 \sim n), (j=1 \sim n-1)$$

本実施形態は、上述したように処理単位ビット長毎に区分けされる複数の部分データに対して元部分データと乱数部分データの排他的論理和演算 (XOR) を行って、詳しくは、元部分データと乱数部分データの排他的論理和演算 (XOR) からなる定義式を用いて、元データの分割を行うことを特徴とするものであり、上述したデータ分割処理に多項式や剰余演算を用いる方法と比較して、コンピュータ処理に適したビット演算である排他的論理和 (XOR) 演算を用いることにより高速かつ高性能な演算処理能力を必要とせず、大容量のデータに対しても簡単な演算処理を繰り返して分割データを生成することができるとともに、また分割データの保管に必要な記憶容量も分割数に比例した倍数の容量よりも小さくすることができる。更に、任意に定めた一定の長さ毎にデータの先頭から順に演算処理を行うストリーム処理により分割データが生成される。

【0097】

次に、フローチャートなどの図面も参照して、本実施の形態における秘密分散法 A の作用について説明するが、この説明の前に図 6 乃至 10、および図 12 に示す記号の定義について説明する。

【0098】

(1) $\Pi_{i=1}^n A(i)$ は、 $A(1) * A(2) * \dots * A(n)$ を意味するものとする。

【0099】

(2) $c(j, i, k)$ を $(n-1) \times (n-1)$ 行列である $U[n-1, n-1] \times (P[n-1, n-1])^{(j-1)}$ の i 行 k 列の値と定義する。

【0100】

このとき $Q(j, i, k)$ を下記のように定義する。

【0101】

$c(j, i, k)=1$ のとき $Q(j, i, k)=R((n-1) \times m+k)$

$c(j, i, k)=0$ のとき $Q(j, i, k)=0$

ただし、 m は $m \geq 0$ の整数を表す。

【0102】

(3) $U[n, n]$ とは、 $n \times n$ 行列であって、 i 行 j 列の値を $u(i, j)$ で表すと、

$i+j \leq n+1$ のとき $u(i, j)=1$

$i+j > n+1$ のとき $u(i, j)=0$

である行列を意味するものとし、「上三角行列」ということとする。具体的には下記のような行列である。

【数 1】

$$U[3, 3] = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \quad U[4, 4] = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

【0103】

(4) $P[n, n]$ とは、 $n \times n$ 行列であって、 i 行 j 列の値を $p(i, j)$ で表すと、

$j=i+1$ のとき $p(i, j)=1$

$i=1, j=n$ のとき $p(i, j)=1$

上記以外るとき $p(i, j)=0$
 である行列を意味するものとし、「回転行列」ということとする。具体的には下記のような行列であり、他の行列の右側からかけると当該他の行列の1列目を2列目へ、2列目を3列目へ、…、 $n-1$ 列目を n 列目へ、 n 列目を1列目へ移動させる作用がある。つまり、行列 P を他の行列に右側から複数回かけると、その回数分だけ各列を右方向へ回転させるように移動させることができる。

【数2】

$$P[3, 3] = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad U[4, 4] = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

【0104】

(5) A, B を $n \times n$ 行列とすると、 $A \times B$ とは行列 A と B の積を意味するものとする。行列の成分同士の計算規則は通常の数学で用いるものと同じである。

【0105】

(6) A を $n \times n$ 行列とし、 i を整数とすると、 A^i とは行列 A の i 個の積を意味するものとする。また、 A^0 とは単位行列 E を意味するものとする。

【0106】

(7) 単位行列 $E[n, n]$ とは、 $n \times n$ 行列であって、 i 行 j 列の値を $e(i, j)$ で表すと、

$i=j$ のとき $e(i, j)=1$

上記以外るとき $e(i, j)=0$

である行列を意味するものとする。具体的には下記のような行列である。 A を任意の $n \times n$ 行列とすると

$$A \times E = E \times A = A$$

となる性質がある。

【数3】

$$E[3, 3] = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad E[4, 4] = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

【0107】

次に、図6に示すフローチャートおよび図7および図8に示す具体的データなどを参照して、まず元データ S の分割処理について説明する。これは、アクセス権管理サーバ5の分割データ生成部52の機能を説明するものである。

【0108】

まず、元データ S をアクセス権管理サーバ5に与える(図6のステップS201)。なお、本例では、元データ S は、16ビットの「10110010 00110111」とする。

【0109】

次に、アクセス権管理サーバ5は、分割数 n として3と指示する(ステップS203)。なお、この分割数 $n=3$ に従ってアクセス権管理サーバ5で生成される3個の分割データを $D(1), D(2), D(3)$ とする。この分割データ $D(1), D(2), D(3)$ は、すべて元データのビット長と同じ16ビット長のデータである。

【0110】

それから、元データSを分割するために使用される処理単位ビット長bを8ビットと決定する(ステップS205)。この処理単位ビット長bは、利用者が端末3からアクセス権管理サーバ5に対して指定してもよいし、またはアクセス権管理サーバ5において予め定められた値を用いてもよい。なお、処理単位ビット長bは、任意のビット数でよいが、ここでは元データSを割り切れることができる8ビットとしている。従って、上記16ビットの「10110010 00110111」の元データSは、8ビットの処理単位ビット長で分けられた場合の2個の元分割データS(1)およびS(2)は、それぞれ「10110010」および「00110111」となる。

【0111】

次のステップS207では、元データSのビット長が 8×2 の整数倍であるか否かを判定し、整数倍でない場合には、元データSの末尾を0で埋めて、 8×2 の整数倍に合わせる。なお、本例のように処理単位ビット長bが8ビットおよび分割数nが3に設定された場合における分割処理は、元データSのビット長として16ビットに限られるものでなく、処理単位ビット長 $b \times (\text{分割数}n-1) = 8 \times 2$ の整数倍の元データSに対して有効なものである。

【0112】

次に、ステップS209では、変数m、すなわち上述した整数倍を意味する変数mを0に設定する。本例のように、元データSが処理単位ビット長 $b \times (\text{分割数}n-1) = 8 \times 2 = 16$ ビットである場合には、変数mは0であるが、2倍の32ビットの場合には、変数mは1となり、3倍の48ビットの場合には、変数mは2となる。

【0113】

次に、元データSの $8 \times 2 \times m + 1$ ビット目から 8×2 ビット分のデータが存在するか否かが判定される(ステップS211)。これは、このステップS211以降に示す分割処理を元データSの変数mで特定される処理単位ビット長 $b \times (\text{分割数}n-1) = 8 \times 2 = 16$ ビットに対して行った後、元データSとして次の16ビットがあるか否かを判定しているものである。本例のように元データSが16ビットである場合には、16ビットの元データSに対してステップS211以降の分割処理を1回行くと、後述するステップS219で変数mが+1されるが、本例の元データSでは変数mがm+1の場合に相当する17ビット以降のデータは存在しないので、ステップS211からステップS221に進むことになるが、今の場合は、変数mは0であるので、元データSの $8 \times 2 \times m + 1$ ビット目は、 $8 \times 2 \times 0 + 1 = 1$ となり、元データSの16ビットの1ビット目から 8×2 ビット分にデータが存在するため、ステップS213に進む。

【0114】

ステップS213では、変数jを1から2(=分割数n-1)まで変えて、元データSの $8 \times (2 \times m + j - 1) + 1$ ビット目から8ビット分(=処理単位ビット長)のデータを元部分データS(2×m+j)に設定し、これにより元データSを処理単位ビット長で分けした2(分割数n-1)個の元部分データS(1), S(2)を次のように生成する。

【0115】

元データS=S(1), S(2)

第1の元部分データS(1)=「10110010」

第2の元部分データS(2)=「00110111」

次に、変数jを1から2(=分割数n-1)まで変えて、乱数部分データR(2×m+j)に乱数生成部51から発生する8ビットの長さの乱数を設定し、これにより乱数Rを処理単位ビット長で分けした2(分割数n-1)個の乱数部分データR(1), R(2)を次のように生成する(ステップS215)。

【0116】

乱数R=R(1), R(2)

第1の乱数部分データR(1)=「10110001」

第2の乱数部分データR(2)=「00110101」

次に、ステップS217において、変数iを1から3(=分割数n)まで変えるとともに、

更に各変数*i*において変数*j*を1から2(=分割数*n*-1)まで変えながら、ステップS 2 1 7に示す分割データを生成するための元部分データと乱数部分データの排他的論理和からなる定義式により複数の分割データ*D(i)*の各々を構成する各分割部分データ*D(i, 2×m+j)*を生成する。この結果、次に示すような分割データ*D*が生成される。

【0 1 1 7】

分割データ*D*

= 3 個の分割データ*D(i)=D(1), D(2), D(3)*

第1の分割データ*D(1)*

= 2 個の分割部分データ*D(1, j)=D(1, 1), D(1, 2)*

= 「00110110」, 「10110011」

第2の分割データ*D(2)*

= 2 個の分割部分データ*D(2, j)=D(2, 1), D(2, 2)*

= 「00000011」, 「00000010」

第3の分割データ*D(3)*

= 2 個の分割部分データ*D(3, j)=D(3, 1), D(3, 2)*

= 「10110001」, 「00110101」

なお、各分割部分データ(*i, j*)を生成するためのステップS 2 1 7に示す定義式は、本例のように分割数*n=3*の場合には、具体的には図8に示す表に記載されているものとなる。図8に示す表から、分割部分データ*D(1, 1)*を生成するための定義式は*S(1)*R(1)*R(2)*であり、*D(1, 2)*の定義式は*S(2)*R(1)*R(2)*であり、*D(2, 1)*の定義式は*S(1)*R(1)*であり、*D(2, 2)*の定義式は*S(2)*R(2)*であり、*D(3, 1)*の定義式は*R(1)*であり、*D(3, 2)*の定義式は*R(2)*である。また、図8に示す表には*m>0*の場合の任意の整数についての一般的な定義式も記載されている。

【0 1 1 8】

このように整数倍を意味する変数*m=0*の場合について分割データ*D*を生成した後、次に変数*m*を1増やし(ステップS 2 1 9)、ステップS 2 1 1に戻り、変数*m+1*に該当する元データ*S*の17ビット以降について同様の分割処理を行おうとするが、本例の元データ*S*は16ビットであり、17ビット以降のデータは存在しないので、ステップS 2 1 1からステップS 2 2 1に進み、上述したように生成した分割データ*D(1), D(2), D(3)*を保管サーバ6及び端末3にそれぞれ保存して、分割処理を終了する。なお、このように保管された分割データ*D(1), D(2), D(3)*はそれぞれ単独では元データが推測できない。

【0 1 1 9】

ここで、上述した図6のフローチャートのステップS 2 1 7における定義式による分割データの生成処理、具体的には分割数*n=3*の場合の分割データの生成処理について詳しく説明する。

【0 1 2 0】

まず、整数倍を意味する変数*m=0*の場合には、ステップS 2 1 7に示す定義式から各分割データ*D(i)=D(1)~D(3)*の各々を構成する各分割部分データ*D(i, 2×m+j)=D(i, j)* (*i=1~3, j=1~2*)は、次のようになる。

【0 1 2 1】

$D(1, 1) = S(1) * Q(1, 1, 1) * Q(1, 1, 2)$

$D(1, 2) = S(2) * Q(2, 1, 1) * Q(2, 1, 2)$

$D(2, 1) = S(1) * Q(1, 2, 1) * Q(1, 2, 2)$

$D(2, 2) = S(2) * Q(2, 2, 1) * Q(2, 2, 2)$

$D(3, 1) = R(1)$

$D(3, 2) = R(2)$

上記の6つの式のうち上から4つの式に含まれる*Q(j, i, k)*を具体的に求める。

【0 1 2 2】

これは*c(j, i, k)*を2×2行列である*U[2, 2] × (P[2, 2])^(j-1)*の*i*行*k*列の値としたとき下記のように定義される。

【 0 1 2 3 】

 $c(j, i, k)=1$ のとき $Q(j, i, k)=R(k)$ $c(j, i, k)=0$ のとき $Q(j, i, k)=0$

ここで、

 $j=1$ のときは

【数 4】

$$U[2, 2] \times (P[2, 2])^{\sim(j-1)} = U[2, 2] \times (P[2, 2])^{\sim 0}$$

$$= U[2, 2] \times E[2, 2]$$

$$= U[2, 2]$$

$$= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

【 0 1 2 4 】

 $j=2$ のときは

【数 5】

$$U[2, 2] \times (P[2, 2])^{\sim(j-1)} = U[2, 2] \times (P[2, 2])^{\sim 1}$$

$$= U[2, 2] \times P[2, 2]$$

$$= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

【 0 1 2 5 】

これを用いると、各分割部分データ $D(i, j)$ は次のような定義式により生成される。

【 0 1 2 6 】

$$D(1, 1)=S(1)*Q(1, 1, 1)*Q(1, 1, 2)=S(1)*R(1)*R(2)$$

$$D(1, 2)=S(2)*Q(2, 1, 1)*Q(2, 1, 2)=S(2)*R(1)*R(2)$$

$$D(2, 1)=S(1)*Q(1, 2, 1)*Q(1, 2, 2)=S(1)*R(1)*0=S(1)*R(1)$$

$$D(2, 2)=S(2)*Q(2, 2, 1)*Q(2, 2, 2)=S(2)*0*R(2)=S(2)*R(2)$$

上述した各分割部分データ $D(i, j)$ を生成するための定義式は、図 7 にも図示されている。

。

【 0 1 2 7 】

図 7 は、上述したように 16 ビットの前データ S を 8 ビットの処理単位ビット長に基づいて分割数 $n=3$ で 3 分割する場合の各データと定義式および各分割部分データから元データを復元する場合の計算式などを示す表である。

【 0 1 2 8 】

ここで、上述した定義式により分割データ $D(1), D(2), D(3)$ および各分割部分データ $D(1, 1), D(1, 2), D(2, 1), D(2, 2), D(3, 1), D(3, 2)$ を生成する過程と定義式の一般形について説明する。

【 0 1 2 9 】

まず、第 1 の分割データ $D(1)$ に対しては、第 1 の分割部分データ $D(1, 1)$ は、上述した定義式 $S(1)*R(1)*R(2)$ で定義され、第 2 の分割部分データ $D(1, 2)$ は定義式 $S(2)*R(1)*R(2)$ で

定義される。なお、この定義式の一般形は、 $D(1, j)$ に対しては $S(j) * R(j) * R(j+1)$ であり、 $D(1, j+1)$ に対して $S(j+1) * R(j) * R(j+1)$ である (j は奇数とする)。定義式に従って計算すると、 $D(1, 1)$ は00110110, $D(1, 2)$ は10110011となるので、 $D(1)$ は00110110 10110011である。なお、定義式の一般形は、図8にまとめて示されている。

【0130】

また、第2の分割データ $D(2)$ に対しては、 $D(2, 1)$ は $S(1) * R(1)$ で定義され、 $D(2, 2)$ は $S(2) * R(2)$ で定義される。この定義式の一般形は、 $D(2, j)$ に対しては $S(j) * R(j)$ であり、 $D(2, j+1)$ に対しては $S(j+1) * R(j+1)$ である (j は奇数とする)。定義式に従って計算すると、 $D(2, 1)$ は00000011, $D(2, 2)$ は00000010となるので、 $D(2)$ は00000011 00000010である。

【0131】

更に第3の分割データ $D(3)$ に対しては、 $D(3, 1)$ は $R(1)$ で定義され、 $D(3, 2)$ は $R(2)$ で定義される。この定義式の一般形は、 $D(3, j)$ に対しては $R(j)$ であり、 $D(3, j+1)$ に対しては $R(j+1)$ である (j は奇数とする)。定義式に従って計算すると、 $D(3, 1)$ は10110001, $D(3, 2)$ は0110101となるので、 $D(3)$ は10110001 0110101である。

【0132】

上記説明は、 $S, R, D(1), D(2), D(3)$ の長さを16ビットとしたが、データの先頭から上記分割処理を繰り返すことにより、どのような長さの元データ S からでも分割データ $D(1), D(2), D(3)$ を生成することができる。また、処理単位ビット長 b は任意にとることができ、元データ S の先頭から順に $b \times 2$ の長さ毎に上記分割処理を繰り返すことにより任意の長さの元データ、具体的には処理単位ビット長 $b \times 2$ の整数倍の長さの元データに対して適用することができる。なお、元データ S の長さが処理単位ビット長 $b \times 2$ の整数倍でない場合は、例えば、データ末尾の部分を0で埋めるなどして元データ S の長さを処理単位ビット長 $b \times 2$ の整数倍に合わせるにより上述した本実施形態の分割処理を適用することができる。

【0133】

次に、図7の右側に示す表を参照して、分割データから元データを復元する処理について説明する。これは、分割データから元データを復元できることを示すものである。

【0134】

まず、アクセス権管理サーバ5に元データ S の復元を要求する。アクセス権管理サーバ5は、保管サーバ6および端末3から分割データ $D(1), D(2), D(3)$ を取得し、この取得した分割データ $D(1), D(2), D(3)$ から次に示すように元データ S を復元する。

【0135】

まず、分割部分データ $D(2, 1), D(3, 1)$ から第1の元部分データ $S(1)$ を次のように生成することができる。

【0136】

$$\begin{aligned} D(2, 1) * D(3, 1) &= (S(1) * R(1)) * R(1) \\ &= S(1) * (R(1) * R(1)) \\ &= S(1) * 0 \\ &= S(1) \end{aligned}$$

具体的に計算すると、 $D(2, 1)$ は00000011, $D(3, 1)$ は10110001なので、 $S(1)$ は10110010となる。

【0137】

また、別の分割部分データから次のように第2の元部分データ $S(2)$ を生成することができる。

【0138】

$$\begin{aligned} D(2, 2) * D(3, 2) &= (S(2) * R(2)) * R(2) \\ &= S(2) * (R(2) * R(2)) \\ &= S(2) * 0 \\ &= S(2) \end{aligned}$$

具体的に計算すると、 $D(2, 2)$ は00000010, $D(3, 2)$ は00110101なので、 $S(2)$ は00110111と

なる。

【0 1 3 9】

一般に、jを奇数として、

$$\begin{aligned} D(2, j) * D(3, j) &= (S(j) * R(j)) * R(j) \\ &= S(j) * (R(j) * R(j)) \\ &= S(j) * 0 \\ &= S(j) \end{aligned}$$

であるから、 $D(2, j) * D(3, j)$ を計算すれば、 $S(j)$ が求まる。

【0 1 4 0】

また、一般に、jを奇数として、

$$\begin{aligned} D(2, j+1) * D(3, j+1) &= (S(j+1) * R(j+1)) * R(j+1) \\ &= S(j+1) * (R(j+1) * R(j+1)) \\ &= S(j+1) * 0 \\ &= S(j+1) \end{aligned}$$

であるから、 $D(2, j+1) * D(3, j+1)$ を計算すれば、 $S(j+1)$ が求まる。

【0 1 4 1】

次に、 $D(1), D(3)$ を取得してSを復元する場合には、次のようになる。

【0 1 4 2】

$$\begin{aligned} D(1, 1) * D(3, 1) * D(3, 2) &= (S(1) * R(1) * R(2)) * R(1) * R(2) = S(1) * (R(1) * R(1)) * (R(2) * R(2)) \\ &= S(1) * 0 * 0 \\ &= S(1) \end{aligned}$$

であるから、 $D(1, 1) * D(3, 1) * D(3, 2)$ を計算すれば、 $S(1)$ が求まる。具体的に計算すると、 $D(1, 1)$ は00110110、 $D(3, 1)$ は10110001、 $D(3, 2)$ は00110101なので、 $S(1)$ は10110010となる。

【0 1 4 3】

また同様に、

$$\begin{aligned} D(1, 2) * D(3, 1) * D(3, 2) &= (S(2) * R(1) * R(2)) * R(1) * R(2) \\ &= S(2) * (R(1) * R(1)) * (R(2) * R(2)) \\ &= S(2) * 0 * 0 \\ &= S(2) \end{aligned}$$

であるから、 $D(1, 2) * D(3, 1) * D(3, 2)$ を計算すれば、 $S(2)$ が求まる。具体的に計算すると、 $D(1, 2)$ は10110011、 $D(3, 1)$ は10110001、 $D(3, 2)$ は00110101なので、 $S(2)$ は00110111となる。

【0 1 4 4】

一般に、jを奇数として、

$$\begin{aligned} D(1, j) * D(3, j) * D(3, j+1) &= (S(j) * R(j) * R(j+1)) * R(j) * R(j+1) \\ &= S(j) * (R(j) * R(j)) * (R(j+1) * R(j+1)) \\ &= S(j) * 0 * 0 \\ &= S(j) \end{aligned}$$

であるから、 $D(1, j) * D(3, j) * D(3, j+1)$ を計算すれば、 $S(j)$ が求まる。

【0 1 4 5】

また、一般に、jを奇数として、

$$\begin{aligned} D(1, j+1) * D(3, j) * D(3, j+1) &= (S(j+1) * R(j) * R(j+1)) * R(j) * R(j+1) \\ &= S(j+1) * (R(j) * R(j)) * (R(j+1) * R(j+1)) \\ &= S(j+1) * 0 * 0 \\ &= S(j+1) \end{aligned}$$

であるから、 $D(1, j+1) * D(3, j) * D(3, j+1)$ を計算すれば、 $S(j+1)$ が求まる。

【0 1 4 6】

次に、 $D(1), D(2)$ を取得してSを復元する場合には、次のようになる。

【0 1 4 7】

$$\begin{aligned}
 D(1,1)*D(2,1) &= (S(1)*R(1)*R(2))*(S(1)*R(1)) \\
 &= (S(1)*S(1))*(R(1)*R(1))*R(2) \\
 &= 0*0*R(2) \\
 &= R(2)
 \end{aligned}$$

であるから、 $D(1,1)*D(2,1)$ を計算すれば、 $R(2)$ が求まる。具体的に計算すると、 $D(1,1)$ は00110110, $D(2,1)$ は00000011なので、 $R(2)$ は00110101となる。

【 0 1 4 8 】

また同様に、

$$\begin{aligned}
 D(1,2)*D(2,2) &= (S(2)*R(1)*R(2))*(S(2)*R(2)) \\
 &= (S(2)*S(2))*R(1)*(R(2)*R(2)) \\
 &= 0*R(1)*0 \\
 &= R(1)
 \end{aligned}$$

であるから、 $D(1,2)*D(2,2)$ を計算すれば、 $R(1)$ が求まる。具体的に計算すると、 $D(1,2)$ は10110011, $D(2,2)$ は00000010なので、 $R(1)$ は10110001となる。

【 0 1 4 9 】

この $R(1), R(2)$ を使用して $S(1), S(2)$ を求める。

【 0 1 5 0 】

$$\begin{aligned}
 D(2,1)*R(1) &= (S(1)*R(1))*R(1) \\
 &= S(1)*(R(1)*R(1)) \\
 &= S(1)*0 \\
 &= S(1)
 \end{aligned}$$

であるから、 $D(2,1)*R(1)$ を計算すれば、 $S(1)$ が求まる。具体的に計算すると、 $D(2,1)$ は00000011, $R(1)$ は10110001なので、 $S(1)$ は10110010となる。

【 0 1 5 1 】

また同様に、

$$\begin{aligned}
 D(2,2)*R(2) &= (S(2)*R(2))*R(2) \\
 &= S(2)*(R(2)*R(2)) \\
 &= S(2)*0 \\
 &= S(2)
 \end{aligned}$$

であるから $D(2,2)*R(2)$ を計算すれば $S(2)$ が求まる。具体的に計算すると $D(2,2)$ は00000010, $R(2)$ は00110101なので、 $S(2)$ は00110111となる。

【 0 1 5 2 】

一般に、 j を奇数として、

$$\begin{aligned}
 D(1,j)*D(2,j) &= (S(j)*R(j)*R(j+1))*(S(j)*R(j)) \\
 &= (S(j)*S(j))*(R(j)*R(j))*R(j+1) \\
 &= 0*0*R(j+1) \\
 &= R(j+1)
 \end{aligned}$$

であるから $D(1,j)*D(2,j)$ を計算すれば $R(j+1)$ が求まる。

【 0 1 5 3 】

また同様に、

$$\begin{aligned}
 D(1,j+1)*D(2,j+1) &= (S(j+1)*R(j)*R(j+1))*(S(j+1)*R(j+1)) \\
 &= (S(j+1)*S(j+1))*R(j)*(R(j+1)*R(j+1)) \\
 &= 0*R(j)*0 \\
 &= R(j)
 \end{aligned}$$

であるから $D(1,j+1)*D(2,j+1)$ を計算すれば $R(j)$ が求まる。

【 0 1 5 4 】

この $R(j), R(j+1)$ を使用して $S(j), S(j+1)$ を求める。

【 0 1 5 5 】

$$\begin{aligned}
 D(2,j)*R(j) &= (S(j)*R(j))*R(j) \\
 &= S(j)*(R(j)*R(j))
 \end{aligned}$$

$$=S(j)*0$$

$$=S(j)$$

であるから $D(2, j)*R(j)$ を計算すれば $S(j)$ が求まる。

【0156】

また同様に、

$$D(2, j+1)*R(j+1)=(S(j+1)*R(j+1))*R(j+1)$$

$$=S(j+1)*(R(j+1)*R(j+1))$$

$$=S(j+1)*0$$

$$=S(j+1)$$

であるから $D(2, j+1)*R(j+1)$ を計算すれば $S(j+1)$ が求まる。

【0157】

上述したように、元データの先頭から処理単位ビット長 b に基づいて分割処理を繰り返して行くと、分割データを生成した場合には、3つの分割データ $D(1), D(2), D(3)$ のすべてを用いなくても、3つの分割データのうち、2つの分割データを用いて上述したように元データを復元することができる。即ち、端末3において、仮に分割データを紛失したとしても、保管サーバ6に保管された他の分割データから元データを復元することができる。

【0158】

尚、本実施の形態に係るアクセス権管理サーバ5においては、3つの分割データ $D(1), D(2), D(3)$ を生成するようになっていたので、分割数が3の場合について説明したが、秘密分散法Aは、分割数が n の場合にも適用できるものである。

【0159】

次に、図9に示すフローチャートを参照して、分割数が n で、処理単位ビット長が b である場合の一般的な分割処理について説明する。

【0160】

まず、元データ S をアクセス権管理サーバ5に与える(ステップS401)。また、アクセス権管理サーバ5に、分割数 n ($n \geq 3$ である任意の整数)を指示する(ステップS403)。処理単位ビット長 b を決定する(ステップS405)。なお、 b は0より大きい任意の整数である。次に、元データ S のビット長が $b \times (n-1)$ の整数倍であるか否かを判定し、整数倍でない場合には、元データ S の末尾を0で埋める(ステップS407)。また、整数倍を意味する変数 m を0に設定する(ステップS409)。

【0161】

次に、元データ S の $b \times (n-1) \times m+1$ ビット目から $b \times (n-1)$ ビット分のデータが存在するか否かが判定される(ステップS411)。この判定の結果、データが存在しない場合は、ステップS421に進むことになるが、今の場合は、ステップS409で変数 m は0に設定された場合であるので、データが存在するため、ステップS413に進む。

【0162】

ステップS413では、変数 j を1から $n-1$ まで変えて、元データ S の $b \times ((n-1) \times m+j-1)+1$ ビット目から b ビット分のデータを元部分データ $S((n-1) \times m+j)$ に設定する処理を繰り返し、これにより元データ S を処理単位ビット長 b で区分けした $(n-1)$ 個の元部分データ $S(1), S(2), \dots, S(n-1)$ が生成される。

【0163】

次に、変数 j を1から $n-1$ まで変えて、乱数部分データ $R((n-1) \times m+j)$ に乱数生成部51から発生する処理単位ビット長 b の乱数を設定し、これにより乱数 R を処理単位ビット長 b で区分けした $n-1$ 個の乱数部分データ $R(1), R(2), \dots, R(n-1)$ が生成される(ステップS415)。

【0164】

次に、ステップS417において、変数 i を1から n まで変えるとともに、更に各変数 i において変数 j を1から $n-1$ まで変えながら、ステップS417に示す分割データを生成するための定義式により複数の分割データ $D(i)$ の各々を構成する各分割部分データ $D(i, (n-1) \times m+j)$ を生成する。この結果、次に示すような分割データ D が生成される。

【0165】

分割データD

=n個の分割データ $D(i)=D(1), D(2), \dots, D(n)$

第1の分割データD(1)

=n-1個の分割部分データ $D(1, j)=D(1, 1), D(1, 2), \dots, D(1, n-1)$

第2の分割データD(2)

=n-1個の分割部分データ $D(2, j)=D(2, 1), D(2, 2), \dots, D(2, n-1)$

...
...
...

第nの分割データD(n)

=n-1個の分割部分データ $D(n, j)=D(n, 1), D(n, 2), \dots, D(n, n-1)$

このように変数 $m=0$ の場合について分割データDを生成した後、次に変数mを1増やし（ステップS419）、ステップS411に戻り、変数 $m=1$ に該当する元データSの $b \times (n-1)$ ビット以降について同様の分割処理を行う。最後にステップS411の判定の結果、元データSにデータがなくなった場合、ステップS411からステップS421に進み、上述したように生成した分割データ $D(1), \dots, D(n)$ を保管サーバ6および端末3にそれぞれ保存して、分割処理を終了する。

【0166】

さて、上述した実施形態においては、ここの分割データのみから、それを構成する部分データ間の演算を行うことによって乱数成分が失われる場合がある。即ち、例えば3分割の場合、各分割部分データは次のように定義される。

【0167】

$D(1, 1)=S(1)*R(1)*R(2), D(1, 2)=S(2)*R(1)*R(2), \dots$

$D(2, 1)=S(1)*R(1), D(2, 2)=S(2)*R(2), \dots$

$D(3, 1)=R(1), D(3, 2)=R(2), \dots$

D(1)について見ると、例えば、 $D(1, 1)$ 、 $D(1, 2)$ が取得できると、

$D(1, 1)*D(1, 2)=(S(1)*R(1)*R(2))*(S(2)*R(1)*R(2))$
 $=S(1)*S(2)*((R(1)*R(1))*(R(2)*R(2)))$
 $=S(1)*S(2)*0*0$
 $=S(1)*S(2)$

となる。一般には $D(1, j)*D(1, j+1)=S(j)*S(j+1)$ である。ここでjは $j=2 \times m+1$ 、mは $m \geq 0$ の任意の整数である。

【0168】

$D(1, 1)$ 、 $D(1, 2)$ は、上記の定義より、元データと乱数の演算により生成されたものであり、 $D(1, 1)$ 、 $D(1, 2)$ それぞれを見ても元データの内容は分からないが、 $D(1, 1)*D(1, 2)$ の演算を行うことにより $S(1)*S(2)$ が算出される。これは元データそのものではないが、乱数成分を含んでいない。

【0169】

このように乱数成分が失われると、個々の元部分データについて、例えばS(2)の一部が既知である場合にはS(1)の一部が復元可能となるので、安全ではないと考えられる。例えば、元データが標準化されたデータフォーマットに従ったデータであって、S(2)がそのデータフォーマット中のヘッダ情報やパディング（例えば、データ領域の一部を0で埋めたもの）などを含む部分であった場合には、これらのデータフォーマット固有のキーワードや固定文字列などを含むため、その内容は予測され得る。また、S(2)のうち既知の部分と $S(1)*S(2)$ の値から、S(1)の一部が復元可能である。

【0170】

この問題を解決する方法は以下の通りである。図10における $D(1, j+1)$ と $D(2, j+1)$ は、図8における $D(1, j+1)$ と $D(2, j+1)$ を入れ替えたものである。ここでjは $j=2 \times m+1$ 、mは $m \geq 0$ の任意の整数である。

【0171】

この場合、個々の分割データのみでは、それを構成する分割部分データ間で演算を行っても乱数成分が失われない。これは、図 10 より

$$\begin{aligned} D(1, j) * D(1, j+1) &= (S(j) * R(j) * R(j+1)) * (S(j+1) * R(j+1)) \\ &= S(j) * S(j+1) * R(j) * (R(j+1) * R(j+1)) \\ &= S(j) * S(j+1) * R(j) * 0 \\ &= S(j) * S(j+1) * R(j) \end{aligned}$$

$$\begin{aligned} D(2, j) * D(2, j+1) &= (S(j) * R(j)) * (S(j+1) * R(j) * R(j+1)) \\ &= S(j) * S(j+1) * (R(j) * R(j)) * R(j+1) \\ &= S(j) * S(j+1) * 0 * R(j+1) \\ &= S(j) * S(j+1) * R(j+1) \end{aligned}$$

$$D(3, j) * D(3, j+1) = R(j) * R(j+1)$$

となるからである。

【0172】

また、この場合、3つの分割データのうち2つから、元データを復元することができるという特性は失われていない。これは、D(1)、D(2)を取得してSを復元する場合には、図 10におけるD(1)、D(2)は、図 8におけるD(1)、D(2)を構成する分割部分データを入れ替えたものにすぎないので、明らかにこれらから元データを復元することができ、また、D(1)とD(3)またはD(2)とD(3)を取得してSを復元する場合には、D(3)は乱数のみからなる分割データであるので、D(1)またはD(2)の分割部分データ毎に必要な個数の乱数との排他的論理和演算を行うことにより、乱数部分を消去して元データを復元することができるからである。

【0173】

次に、一旦分割された分割データにさらに乱数を与えて新たな分割データ（再分割データ）を生成する再分割処理について説明する。これは、アクセス権管理サーバ5の再分割データ生成部53の機能を説明するものであるが、これに関しても、分割数が3の場合を例に説明する。

【0174】

図 11は、データ再分割処理の概要を説明するフローチャート図である。同図によれば、まず分割データD(1)、D(2)、D(3)を取得し（ステップS601）、次に、乱数生成部51で再分割の際に用いる乱数R'を発生させる（ステップS603）。

【0175】

次に、分割データD(1)、D(2)、D(3)それぞれに乱数R'を所定のルールで注入する（ステップS605）。これは、後述するようなルールにより分割データD(1)、D(2)、D(3)の分割部分データと乱数R'の乱数部分データの排他的論理和をとり、分割データから旧乱数であるRを消去して、新たな分割データD'(1)、D'(2)、D'(3)を生成するものである（ステップS607、S609）。

【0176】

図 12は、元データSを、元データの半分の長さの処理単位ビット長bに基づいて分割数n=3で3分割する場合の分割部分データの定義式、乱数R'の再注入後の分割部分データの定義式、さらに乱数Rを消去後の分割部分データの定義式および各分割部分データから元データを復元する場合の計算式などを示す表である。

【0177】

ここで、分割部分データD(i, j)の定義式について説明する。

【0178】

まず、第1の分割データD(1)に対しては、図 10に示すように、第1の分割部分データD(1, 1)は、定義式S(1)*R(1)*R(2)で定義され、第2の分割部分データD(1, 2)は定義式S(2)*R(2)で定義される。なお、この定義式の一般形は、D(1, j)に対してはS(j)*R(j)*R(j+1)であり、D(1, j+1)に対してS(j+1)*R(j+1)である（jは奇数とする）。

【0179】

また、第2の分割データD(2)に対しては、図 10に示すように、D(2, 1)はS(1)*R(1)で

定義され、 $D(2, 2)$ は $S(2)*R(1)*R(2)$ で定義される。この定義式の一般形は、 $D(2, j)$ に対しては $S(j)*R(j)$ であり、 $D(2, j+1)$ に対しては $S(j+1)*R(j)*R(j+1)$ である (j は奇数とする)。

【0180】

更に第3の分割データ $D(3)$ に対しては、図10に示すように、 $D(3, 1)$ は $R(1)$ で定義され、 $D(3, 2)$ は $R(2)$ で定義される。この定義式の一般形は、 $D(3, j)$ に対しては $R(j)$ であり、 $D(3, j+1)$ に対しては $R(j+1)$ である (j は奇数とする)。

【0181】

次に、新たな乱数 R' 注入後の分割部分データ $D' (i, j)$ の定義式について説明する。

【0182】

まず、第1の分割データ $D' (1)$ に対しては、図12に示すように、第1の分割部分データ $D' (1, 1)$ は、定義式 $D(1, 1)*R' (1)*R' (2)$ 、即ち、 $S(1)*R(1)*R(2)*R' (1)*R' (2)$ で定義され、第2の分割部分データ $D' (1, 2)$ は、定義式 $D(1, 2)*R' (2)$ 、即ち、 $S(2)*R(2)*R' (2)$ で定義される。なお、この定義式の一般形は、 $D' (1, j)$ に対しては $D(1, j)*R' (j)*R' (j+1)$ であり、 $D' (1, j+1)$ に対しては $D(1, j+1)*R' (j+1)$ である (j は奇数とする)。

【0183】

また、第2の分割データ $D' (2)$ に対しては、図12に示すように、 $D' (2, 1)$ は $D(2, 1)*R' (1)$ 、即ち、 $S(1)*R(1)*R' (1)$ で定義され、 $D' (2, 2)$ は $D(2, 2)*R' (1)*R' (2)$ 、即ち、 $S(2)*R(1)*R(2)*R' (1)*R' (2)$ で定義される。この定義式の一般形は、 $D' (2, j)$ に対しては $D(2, j)*R' (j)$ であり、 $D' (2, j+1)$ に対しては $D(2, j+1)*R' (j)*R' (j+1)$ である (j は奇数とする)。

【0184】

また、第3の分割データ $D' (3)$ に対しては、図12に示すように、 $D' (3, 1)$ は $D(3, 1)*R' (1)$ 、即ち、 $R(1)*R' (1)$ で定義され、 $D' (3, 2)$ は $D(3, 2)*R' (2)$ 、即ち、 $R(2)*R' (2)$ で定義される。この定義式の一般形は、 $D' (3, j)$ に対しては $D(3, j)*R' (j)$ であり、 $D' (3, j+1)$ に対しては $D(3, j+1)*R' (j+1)$ である (j は奇数とする)。

【0185】

次に、古い乱数 R を消去した分割部分データの定義式について説明する。

【0186】

まず、上述の第1の分割データ $D' (1)$ に対しては、図12に示すように、第1の分割部分データ $D' (1, 1)$ は、定義式 $(S(1)*R(1)*R(2)*R' (1)*R' (2))*(R(1)*R(2))$ 、即ち、 $S(1)*R' (1)*R' (2)$ で定義され、第2の分割部分データ $D' (1, 2)$ は、定義式 $(S(2)*R(2)*R' (2))*R(2)$ 、即ち、 $S(2)*R' (2)$ で定義される。なお、この定義式の一般形は、 $D' (1, j)$ に対しては $S(j)*R' (j)*R' (j+1)$ であり、 $D' (1, j+1)$ に対しては $S(j+1)*R' (j+1)$ である (j は奇数とする)。

【0187】

また、上述の第2の分割データ $D' (2)$ に対しては、図12に示すように、 $D' (2, 1)$ は $(S(1)*R(1)*R' (1))*R(1)$ 、即ち、 $S(1)*R' (1)$ で定義され、 $D' (2, 2)$ は $(S(2)*R(1)*R(2))*R' (1)*R' (2)$ 、即ち、 $S(2)*R' (1)*R' (2)$ で定義される。この定義式の一般形は、 $D' (2, j)$ に対しては $S(j)*R' (j)$ であり、 $D(2, j+1)$ に対しては $S(j+1)*R' (j)*R' (j+1)$ である (j は奇数とする)。

【0188】

また、上述の第3の分割データ $D' (3)$ に対しては、図12に示すように、 $D' (3, 1)$ は $(R(1)*R' (1))*R(1)$ 、即ち、 $R' (1)$ で定義され、 $D' (3, 2)$ は $(R(2)*R' (2))*R(2)$ 、即ち、 $R' (2)$ で定義される。この定義式の一般形は、 $D' (3, j)$ に対しては $R' (j)$ であり、 $D(3, j+1)$ に対しては $R' (j+1)$ である (j は奇数とする)。

【0189】

このように、再分割部分データ $D' (i, j)$ はそれぞれ、分割部分データ $D (i, j)$ に、分割部分データ $D (i, j)$ の定義式で注入されていた乱数部分データ $R(j)$ に対応する乱数部分データ $R' (j)$ を注入した後、さらに乱数部分データ $R(j)$ を消去するように乱数部分データ R (

j)を注入して排他的論理和を計算し、求めるものである。

【0190】

その結果、もとの分割部分データD (i, j)の定義式において、乱数部分データR(j)を乱数部分データR' (j)に置換したものが、再分割部分データD' (i, j)の定義式となる。

【0191】

次に、図12の右側に示す表を参照して、再分割データから元データを復元する処理について説明する。これは、アクセス権管理サーバ5の元データ復元部54の機能を説明するものである。

【0192】

まず、分割部分データD' (2, 1), D' (3, 1)から第1の元部分データS(1)を次のように生成することができる。

【0193】

$$\begin{aligned} D' (2, 1) * D' (3, 1) &= (S(1) * R' (1)) * R' (1) \\ &= S(1) * (R' (1) * R' (1)) \\ &= S(1) * 0 \\ &= S(1) \end{aligned}$$

また、別の分割部分データから次のように第2の元部分データS(2)を生成することができる。

【0194】

$$\begin{aligned} D' (2, 2) * D' (3, 1) * D' (3, 2) &= (S(2) * R' (1) * R' (2)) * R' (1) * R' (2) \\ &= S(2) * (R' (1) * R' (1)) * (R' (2) * R' (2)) \\ &= S(2) * 0 * 0 \\ &= S(2) \end{aligned}$$

一般に、jを奇数として、

$$\begin{aligned} D' (2, j) * D' (3, j) &= (S(j) * R' (j)) * R' (j) \\ &= S(j) * (R' (j) * R' (j)) \\ &= S(j) * 0 \\ &= S(j) \end{aligned}$$

であるから、D' (2, j) * D' (3, j)を計算すれば、S(j)が求まる。

【0195】

また、一般に、jを奇数として、

$$\begin{aligned} D' (2, j+1) * D' (3, j) * D' (3, j+1) &= (S(j+1) * R' (j) * R' (j+1)) * R' (j) * R' (j+1) \\ &= S(j+1) * (R' (j) * R' (j)) * (R' (j+1) * R' (j+1)) \\ &= S(j+1) * 0 * 0 \\ &= S(j+1) \end{aligned}$$

であるから、D' (2, j+1) * D' (3, j) * D' (3, j+1)を計算すれば、S(j+1)が求まる。

【0196】

次に、D' (1), D' (3)を取得してSを復元する場合には、次のようになる。

【0197】

$$\begin{aligned} D' (1, 1) * D' (3, 1) * D' (3, 2) &= (S(1) * R' (1) * R' (2)) * R' (1) * R' (2) \\ &= S(1) * (R' (1) * R' (1)) * (R' (2) * R' (2)) \\ &= S(1) * 0 * 0 \\ &= S(1) \end{aligned}$$

であるから、D' (1, 1) * D' (3, 1) * D' (3, 2)を計算すれば、S(1)が求まる。

【0198】

また同様に、

$$\begin{aligned} D' (1, 2) * D' (3, 2) &= (S(2) * R' (2)) * R' (2) \\ &= S(2) * (R' (2) * R' (2)) \\ &= S(2) * 0 \\ &= S(2) \end{aligned}$$

であるから、 $D'(1,2) * D'(3,2)$ を計算すれば、 $S(2)$ が求まる。

【0 1 9 9】

一般に、 j を奇数として、

$$\begin{aligned} D'(1,j) * D'(3,j) * D'(3,j+1) &= (S(j) * R'(j) * R'(j+1)) * R'(j) * R'(j+1) \\ &= S(j) * (R'(j) * R'(j)) * (R'(j+1) * R'(j+1)) \\ &= S(j) * 0 * 0 \\ &= S(j) \end{aligned}$$

であるから、 $D'(1,j) * D'(3,j) * D'(3,j+1)$ を計算すれば、 $S(j)$ が求まる。

【0 2 0 0】

また、一般に、 j を奇数として、

$$\begin{aligned} D'(1,j+1) * D'(3,j+1) &= (S(j+1) * R'(j+1)) * R'(j+1) \\ &= S(j+1) * (R'(j+1) * R'(j+1)) \\ &= S(j+1) * 0 \\ &= S(j+1) \end{aligned}$$

であるから、 $D'(1,j+1) * D'(3,j+1)$ を計算すれば、 $S(j+1)$ が求まる。

【0 2 0 1】

次に、 $D'(1), D'(2)$ を取得して S を復元する場合には、次のようになる。

【0 2 0 2】

$$\begin{aligned} D'(1,1) * D'(2,1) &= (S(1) * R'(1) * R'(2)) * (S(1) * R'(1)) \\ &= (S(1) * S(1)) * (R'(1) * R'(1)) * R'(2) \\ &= 0 * 0 * R'(2) \\ &= R'(2) \end{aligned}$$

であるから、 $D'(1,1) * D'(2,1)$ を計算すれば、 $R'(2)$ が求まる。

【0 2 0 3】

また同様に、

$$\begin{aligned} D'(1,2) * D'(2,2) &= (S(2) * R'(2)) * (S(2) * R'(1) * R'(2)) \\ &= (S(2) * S(2)) * (R'(2) * R'(2)) * R'(1) \\ &= 0 * 0 * R'(1) \\ &= R'(1) \end{aligned}$$

であるから、 $D'(1,2) * D'(2,2)$ を計算すれば、 $R'(1)$ が求まる。

【0 2 0 4】

この $R'(1), R'(2)$ を使用して $S(1), S(2)$ を求める。

【0 2 0 5】

$$\begin{aligned} D'(2,1) * R'(1) &= (S(1) * R'(1)) * R'(1) \\ &= S(1) * (R'(1) * R'(1)) \\ &= S(1) * 0 \\ &= S(1) \end{aligned}$$

であるから、 $D'(2,1) * R'(1)$ を計算すれば、 $S(1)$ が求まる。

【0 2 0 6】

また同様に、

$$\begin{aligned} D'(1,2) * R'(2) &= (S(2) * R'(2)) * R'(2) \\ &= S(2) * (R'(2) * R'(2)) \\ &= S(2) * 0 \\ &= S(2) \end{aligned}$$

であるから $D'(1,2) * R'(2)$ を計算すれば $S(2)$ が求まる。

【0 2 0 7】

一般に、 j を奇数として、

$$\begin{aligned} D'(1,j) * D'(2,j) &= (S(j) * R'(j) * R'(j+1)) * (S(j) * R'(j)) \\ &= (S(j) * S(j)) * (R'(j) * R'(j)) * R'(j+1) \\ &= 0 * 0 * R'(j+1) \end{aligned}$$

$$= R' (j+1)$$

であるから $D' (1, j) * D' (2, j)$ を計算すれば $R' (j+1)$ が求まる。

【0208】

また同様に、

$$\begin{aligned} D' (1, j+1) * D' (2, j+1) &= (S(j+1) * R' (j+1)) * (S(j+1) * R' (j) * R' (j+1)) \\ &= (S(j+1) * S(j+1)) * (R' (j+1) * R' (j+1)) * R' (j) \\ &= 0 * 0 * R' (j) \\ &= R' (j) \end{aligned}$$

であるから $D' (1, j+1) * D' (2, j+1)$ を計算すれば $R' (j)$ が求まる。

【0209】

この $R' (j)$, $R' (j+1)$ を使用して $S(j)$, $S(j+1)$ を求める。

【0210】

$$\begin{aligned} D' (2, j) * R' (j) &= (S(j) * R' (j)) * R' (j) \\ &= S(j) * (R' (j) * R' (j)) \\ &= S(j) * 0 \\ &= S(j) \end{aligned}$$

であるから $D' (2, j) * R' (j)$ を計算すれば $S(j)$ が求まる。

【0211】

また同様に、

$$\begin{aligned} D' (1, j+1) * R' (j+1) &= (S(j+1) * R' (j+1)) * R' (j+1) \\ &= S(j+1) * (R' (j+1) * R' (j+1)) \\ &= S(j+1) * 0 \\ &= S(j+1) \end{aligned}$$

であるから $D' (1, j+1) * R' (j+1)$ を計算すれば $S(j+1)$ が求まる。

【0212】

以上、再分割データを生成した場合には、3つの再分割データ $D' (1)$, $D' (2)$, $D' (3)$ のすべてを用いなくても、3つの再分割データのうち、2つの再分割データを用いて上述したように元データを復元することができる。

【0213】

また、このデータ再分割方法においては、一旦元データを復元することなく（元データが見える形で現れない）、データの再分割処理を行うことができるので、よりセキュアなデータ管理が可能となる。

【0214】

(動作)

次に、本実施の形態に係るアクセス権管理システム30の動作を図13を用いて説明する。ここで、図13は、データSのデータ権限を甲から乙に譲渡するときの端末3a、端末3bとアクセス権管理サーバ5間のデータのやりとりを示すシーケンス図である。

【0215】

まず、甲がデータSのアクセス権限を有する場合には、データSを甲の端末3aからアクセス管理サーバ5に送信する（ステップS410）。尚、データSの送信に際しては、通信内容の漏洩を防止するセキュアな通信ネットワーク2a（例えば、インターネット網などのオープンな通信ネットワーク2bではなく、LAN、IP-VPN、専用線、電話回線など）を用いる、また、通信ネットワーク2aを介した通信ではなく、例えば、郵便などの送付手段を用いてもよい。

【0216】

アクセス権管理サーバ5は、端末3aからデータSを受け取ると、甲の乱数Rを生成し、上述した秘密分散法Aを用いて3つのデータ（分割データ） $D(1)$, $D(2)$, $D(3)$ を生成する（ステップS420, S430）。例えば、具体的には、

$$\begin{aligned} D(1) &= (S(1) * R(1) * R(2)) \parallel (S(2) * R(2)) \\ D(2) &= (S(1) * R(1)) \parallel (S(2) * R(1) * R(2)) \end{aligned}$$

$D(3) = R(1) \parallel R(2)$

ただし、 \parallel は、ビット列とビット列との結合を意味する。

【0217】

次に、アクセス権管理サーバ5は、分割データD(1),D(2)を保管サーバ6a, 6bにそれぞれ保管するとともに、分割データD(3)を通信ネットワーク2を介して甲の端末3aに送信する(ステップS440, S450)。尚、分割データD(3)は、上述したように、 $D(3) = R(1) \parallel R(2)$ であるため、分割データD(3)の送信は、乱数Rの送信と同じことである。

【0218】

端末3aは、アクセス権管理サーバ5から分割データD(3)を受け取ると、分割データD(3)を記憶部31に記憶させる(ステップS460)。

【0219】

以上の動作により、甲のデータSに対するアクセス権限は、アクセス権管理サーバ5で管理されることになる。

【0220】

次に、甲がデータSのアクセス権限を乙に譲渡する場合には、甲から乙へのデータのアクセス権譲渡の要求、及び分割データD(3)を、甲の端末3aから通信ネットワーク2を介してアクセス権管理サーバ5に送信する(ステップS510)。

【0221】

アクセス権管理サーバ5は、端末3aから甲から乙へのアクセス権譲渡要求、及び分割データD(3)を受け取ると、乙の乱数R'を生成し、分割データD(1),D(2),D(3)から秘密分散法Aを用いて、新たに3つのデータ(再分割データ)D'(1),D'(2),D'(3)を生成する(ステップS520, S530)。例えば、具体的には、

$D'(1) = (S(1)*R'(1)*R'(2)) \parallel (S(2)*R'(2))$

$D'(2) = (S(1)*R'(1)) \parallel (S(2)*R'(1)*R'(2))$

$D'(3) = R'(1) \parallel R'(2)$

次に、アクセス権管理サーバ5は、再分割データD'(1),D'(2)を保管サーバ6a, 6bにそれぞれ保管するとともに、再分割データD'(3)を通信ネットワーク2を介して乙の端末3bに送信する(ステップS540, S550)。尚、再分割データD'(3)は、上述したように、 $D'(3) = R'(1) \parallel R'(2)$ であるため、分割データD'(3)の送信は、乱数R'の送信と同じことである。

【0222】

端末3bは、アクセス権管理サーバ5から再分割データD'(3)を受け取ると、再分割データD'(3)を記憶部31に記憶させる(ステップS560)。

【0223】

以上の動作により、データSに対するアクセス権限は、甲から乙に譲渡されたことになる。

【0224】

次に、乙がデータSを使用する場合には、データSの使用要求、及び再分割データD'(3)を端末3bから通信ネットワーク2を介してアクセス管理サーバ5に送信する(ステップS610)。

【0225】

アクセス権管理サーバ5は、端末3bからデータSの使用要求、及び再分割データD'(3)を受け取ると、保管サーバ6a, 6bに保管された再分割データD'(1), D'(2)を取得し、これら再分割データD'(1), D'(2), D'(3)のうち、任意の2つから秘密分散法Aを用いて、データSを復号する(ステップS620)。

【0226】

次に、アクセス権管理サーバ5は、復号されたデータSをセキュアな通信ネットワーク2a又は送付手段を介して乙の端末3bに送信する(ステップS630)。

【0227】

端末3bは、アクセス管理サーバ5からデータSを受け取ると、データSを記憶部31

に記憶させる（ステップS640）。これにより、乙はデータSを端末3bで使うことができる。

【0228】

従って、本実施の形態に係るアクセス権管理システム30によれば、秘密分散法Aを用いて暗号化するアクセス権管理サーバ5、並びに端末3a及び3bを備え、アクセス権管理サーバ5は、データのアクセス権限を譲渡する譲渡側の端末3aのユーザ甲のデータSを甲の乱数Rを用いて秘密分散法Aにより、分割データを生成し、該分割データの一部を端末3a、残りをアクセス権管理サーバ5で管理する。そして、甲から譲受側の端末3bのユーザ乙にデータSのアクセス権限が譲渡された場合には、アクセス権管理サーバ5は、乙の乱数R'を用いて分割データから秘密分散法Aにより再分割データを生成し、該再分割データの一部を端末3b、残りをアクセス権管理サーバ5で管理するので、暗号化によりアクセス制限されたデータのアクセス権限を他人に譲渡する場合であっても、一旦復号せずにデータ権限を譲渡でき、セキュリティを十分に確保することができる。

【0229】

特に、本発明における秘密分散法Aは、データを所望の処理単位ビット長に基づいて所望の分割数の分割データに分割するデータ分割方法であり、データを処理単位ビット長毎に区別して、複数の元部分データを生成し、この複数の元部分データの各々に対応して、データのビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成して、所望の分割数の分割データを生成するとともに、生成した分割データのうちの所定の個数の分割データからデータが復元することができ、また、新たに発生させた乱数から処理単位ビット長の複数の乱数部分データを生成し、各分割部分データと該乱数部分データの排他的論理和により処理単位ビット長毎に再分割部分データを生成して、所望の分割数の再分割データを生成するとともに、生成した再分割データのうちの所定の個数の再分割データからデータが復元することができるので、データを復元することなく、データを再分割することができる。

【0230】

これにより、ユーザのデータをよりセキュアに管理することができる。

尚、本実施の形態における秘密分散法Aは、多項式演算・剰余演算などを含む多倍長整数の演算処理を必要としないので、大容量データを多数処理する場合においても簡単かつ迅速にデータの分割および復元を行うことができるという効果を得ることができる。

【図面の簡単な説明】

【0231】

【図1】本発明の第1の実施の形態に係るアクセス権管理システムの概略構成を示すブロック図である。

【図2】本発明の第1の実施の形態に係るアクセス権管理システムの動作を示すシーケンス図である。

【図3】本発明の第2の実施の形態に係るアクセス権管理システムの概略構成を示すブロック図である。

【図4】本発明の第2の実施の形態に係るアクセス権管理システムの動作を示すシーケンス図である。

【図5】本発明の第3の実施の形態に係るアクセス権管理システムの概略構成を示すブロック図である。

【図6】秘密分散法Aの分割数 $n=3$ の場合の分割処理を示すフローチャートである。

【図7】16ビットの元データSを8ビットの処理単位ビット長に基づいて分割数 $n=3$ で3分割する場合の各データと定義式および各分割部分データから元データを復元する場合の計算式などを示す表である。

【図8】分割数 $n=3$ の場合の分割データ、分割部分データ、各分割部分データを生成



する定義式を示す表である。

【図 9】秘密分散法 A の分割数が n で処理単位ビット長が b である場合の一般的な分割処理を示すフローチャートである。

【図 10】分割数 $n=3$ の場合の分割データ、分割部分データ、各分割部分データを生成する定義式の別の例を示す表である。

【図 11】秘密分散法 A のデータ再分割処理を示すフローチャートである。

【図 12】乱数書き換え方式により元データ S を元データ S の半分の長さの処理単位ビット長に基づいて分割数 $n=3$ で再分割する場合の各データと定義式および各分割部分データから元データを復元する場合の計算式などを示す表である。

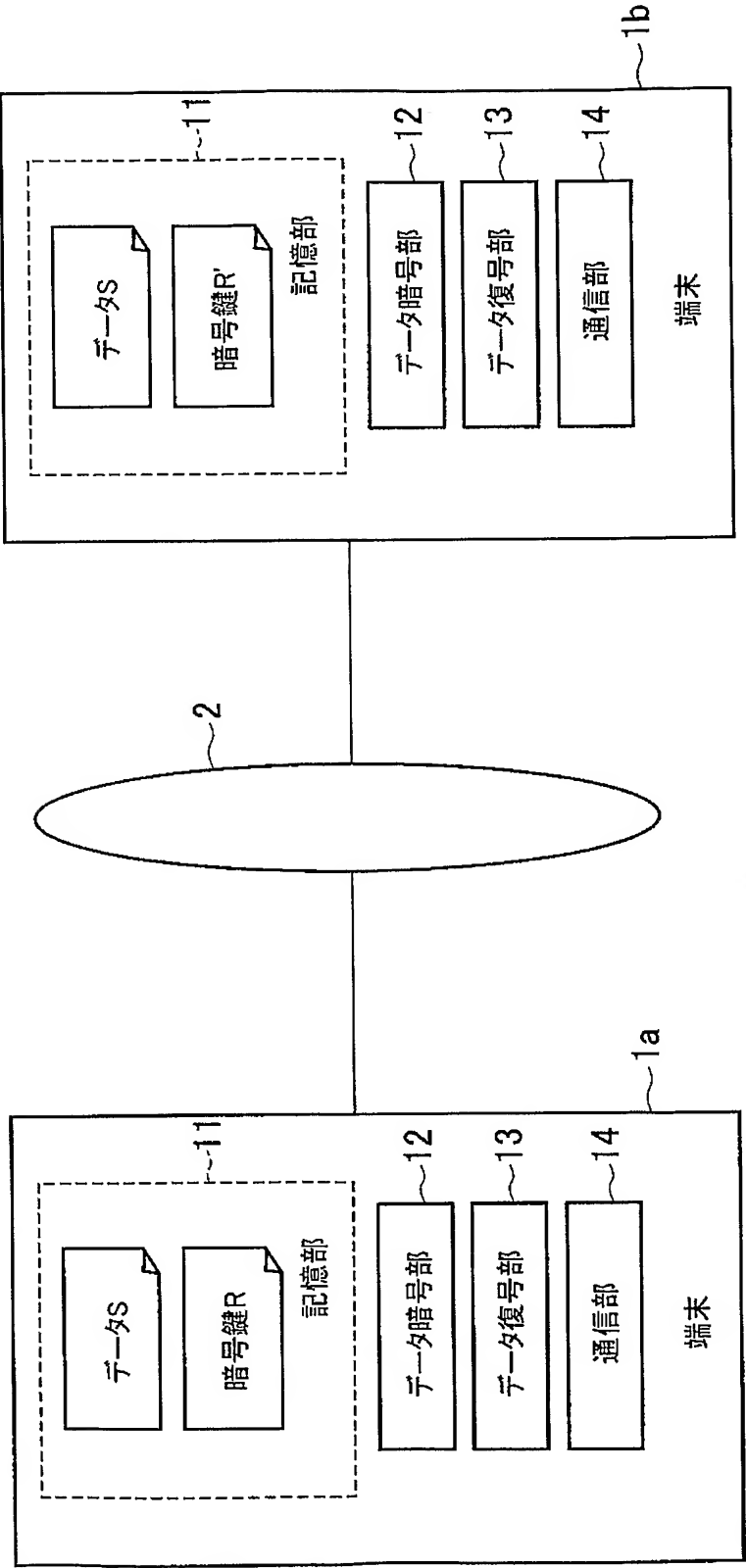
【図 13】本発明の第 3 の実施の形態に係るアクセス権管理システムの動作を示すシーケンス図である。

【符号の説明】

【0232】

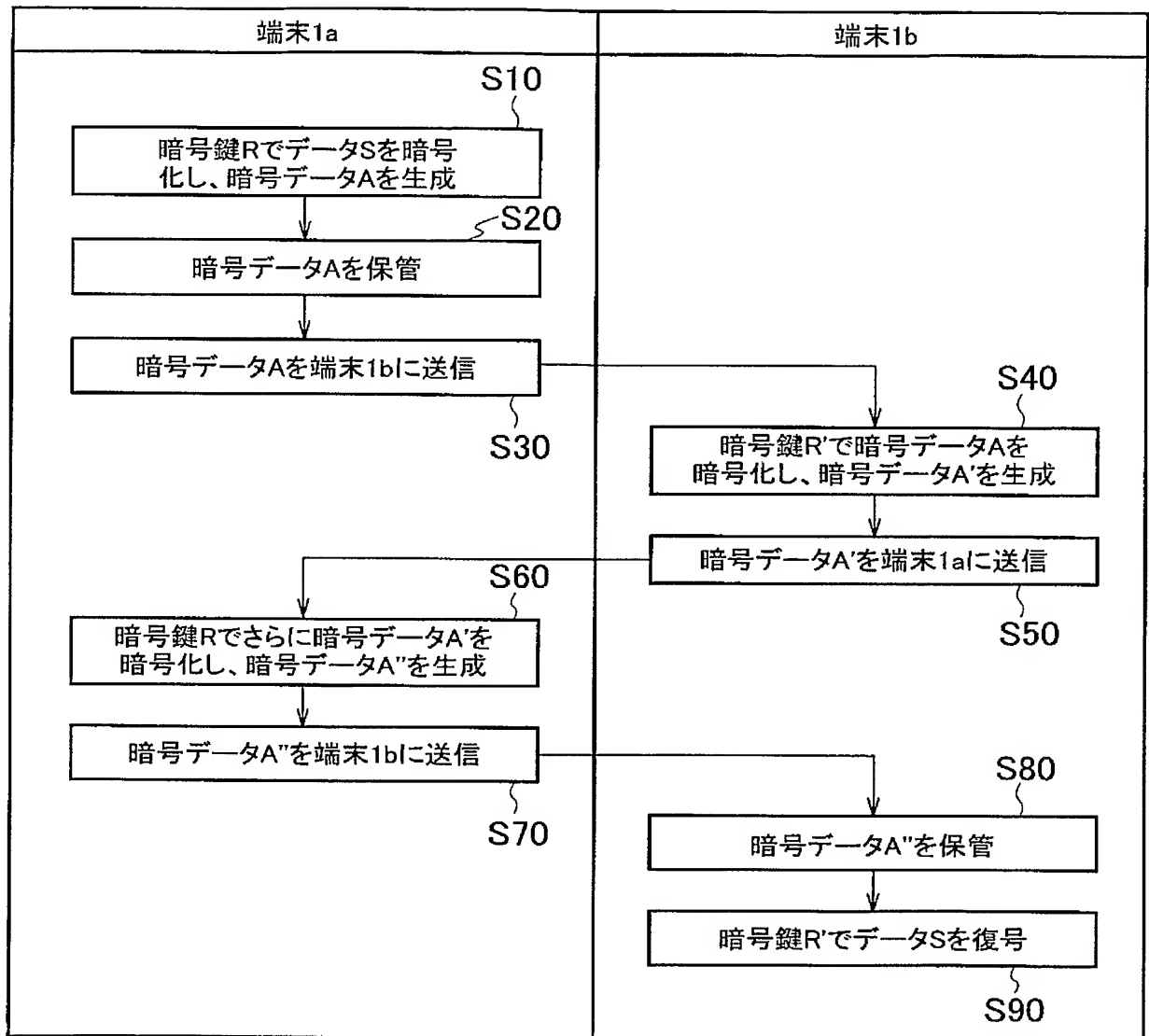
- 1 a, 1 b, 3 a, 3 b…端末
- 2…通信ネットワーク
- 4, 5…アクセス権管理サーバ
- 6 a, 6 b…保管サーバ
- 10, 20, 30…アクセス権管理システム
- 11, 31…記憶部
- 12…データ暗号部
- 13…データ復号部
- 14, 32…通信部
- 41…暗号データ記憶部
- 42…鍵生成部
- 43…データ暗号部
- 44…データ復号部
- 45…通信部

【書類名】 図面
【図 1】

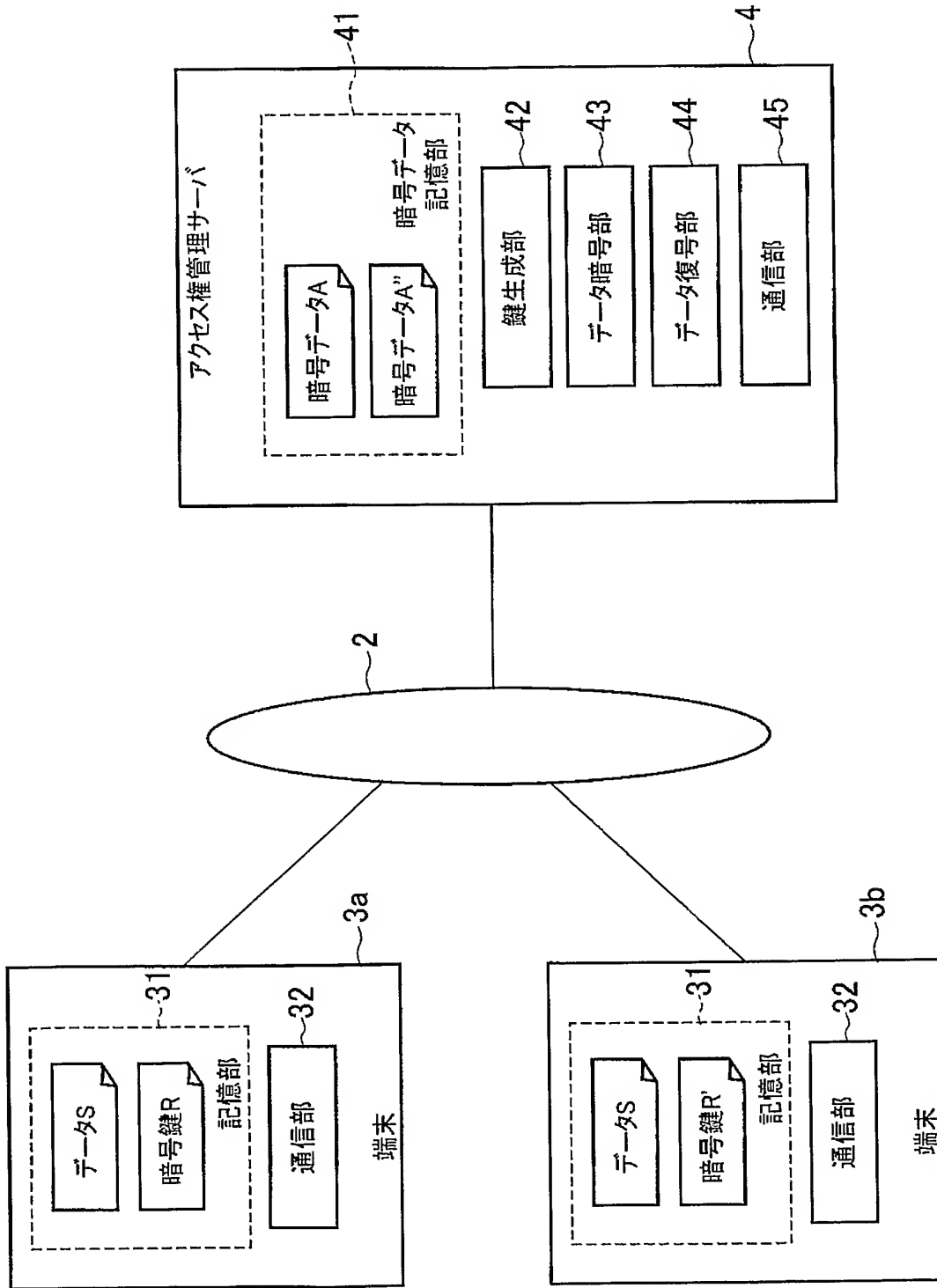


10 アクセス権管理システム

【図 2】

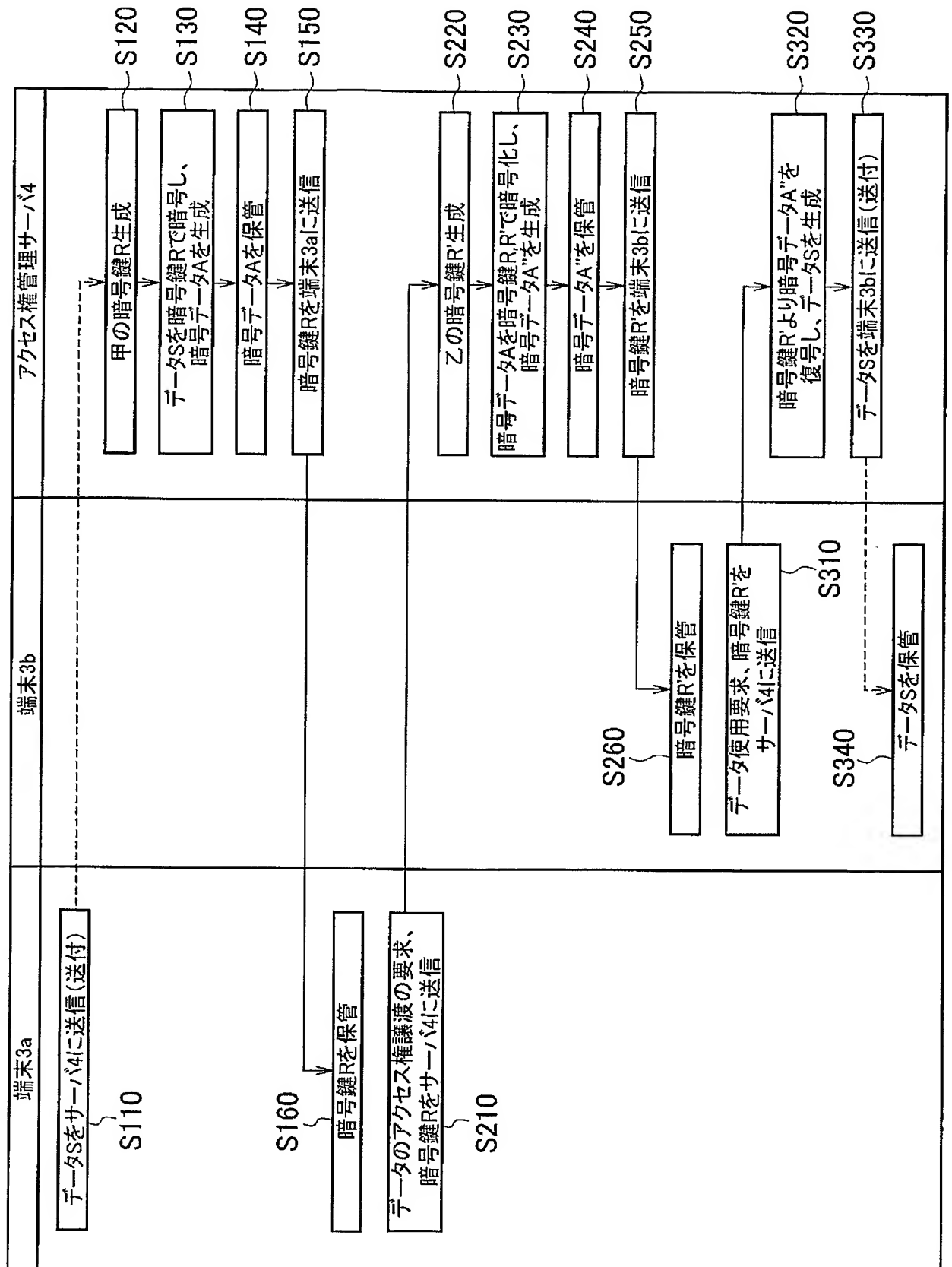


【図 3】

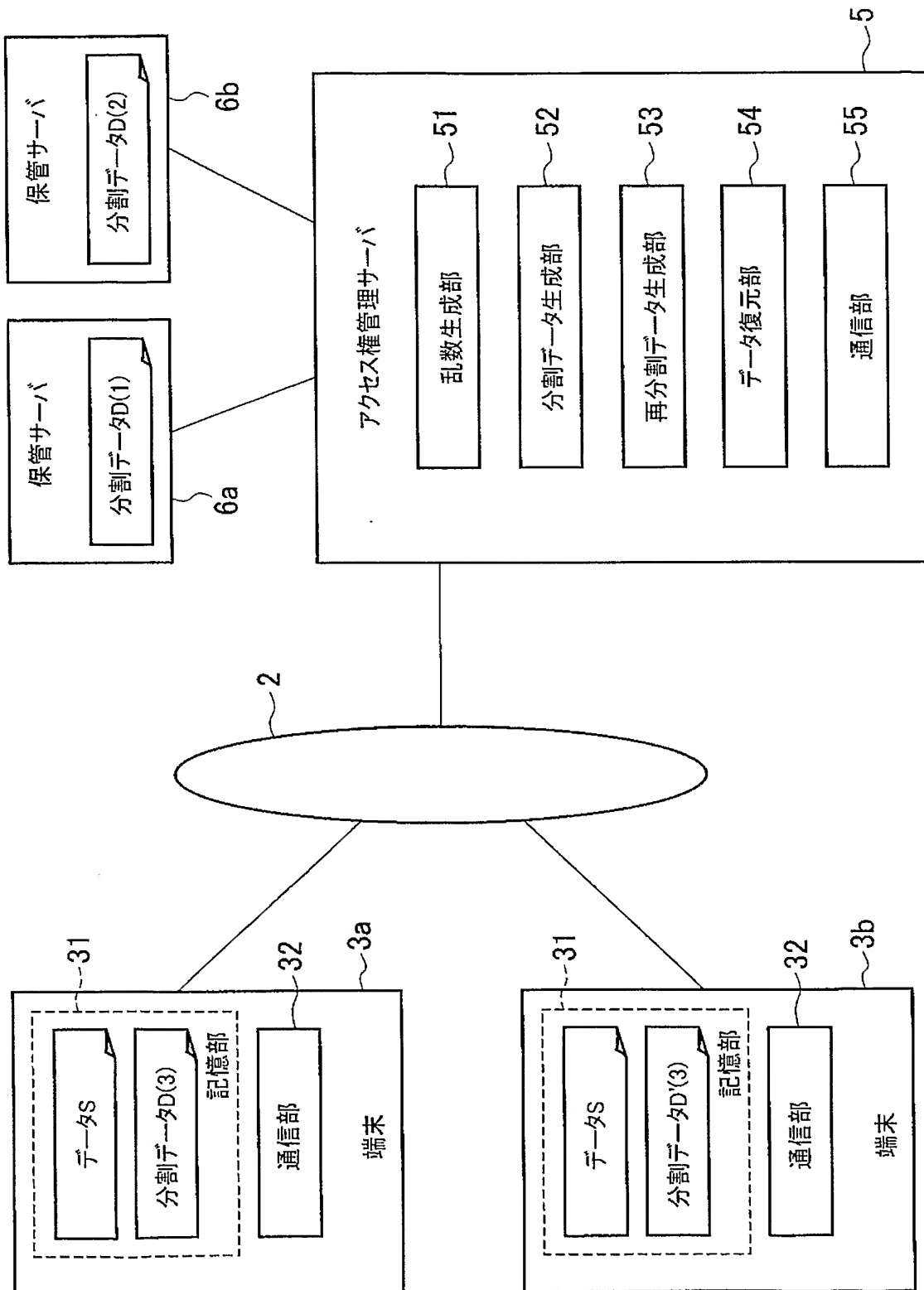


20 アクセス権管理システム

【図 4】

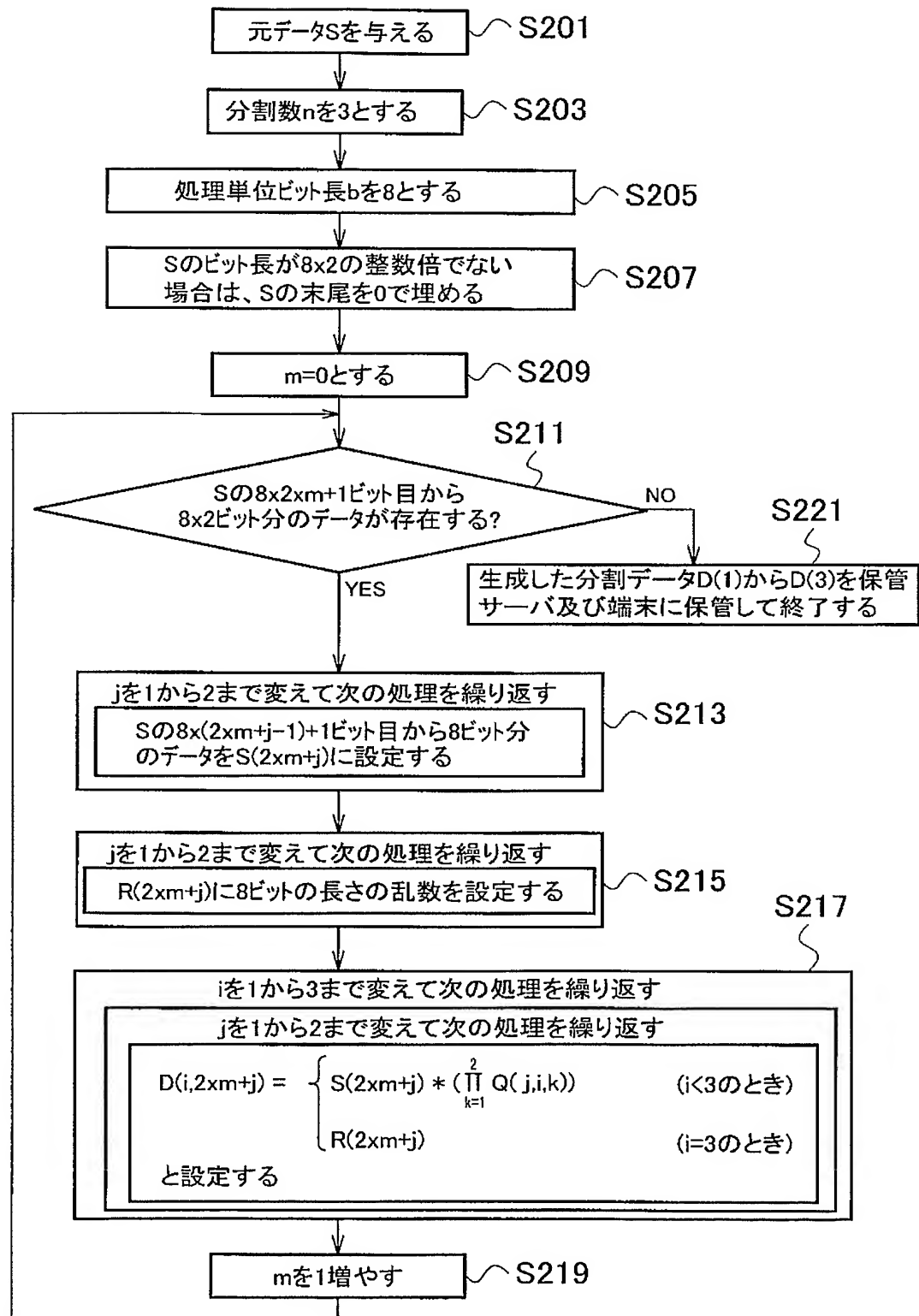


【図 5】



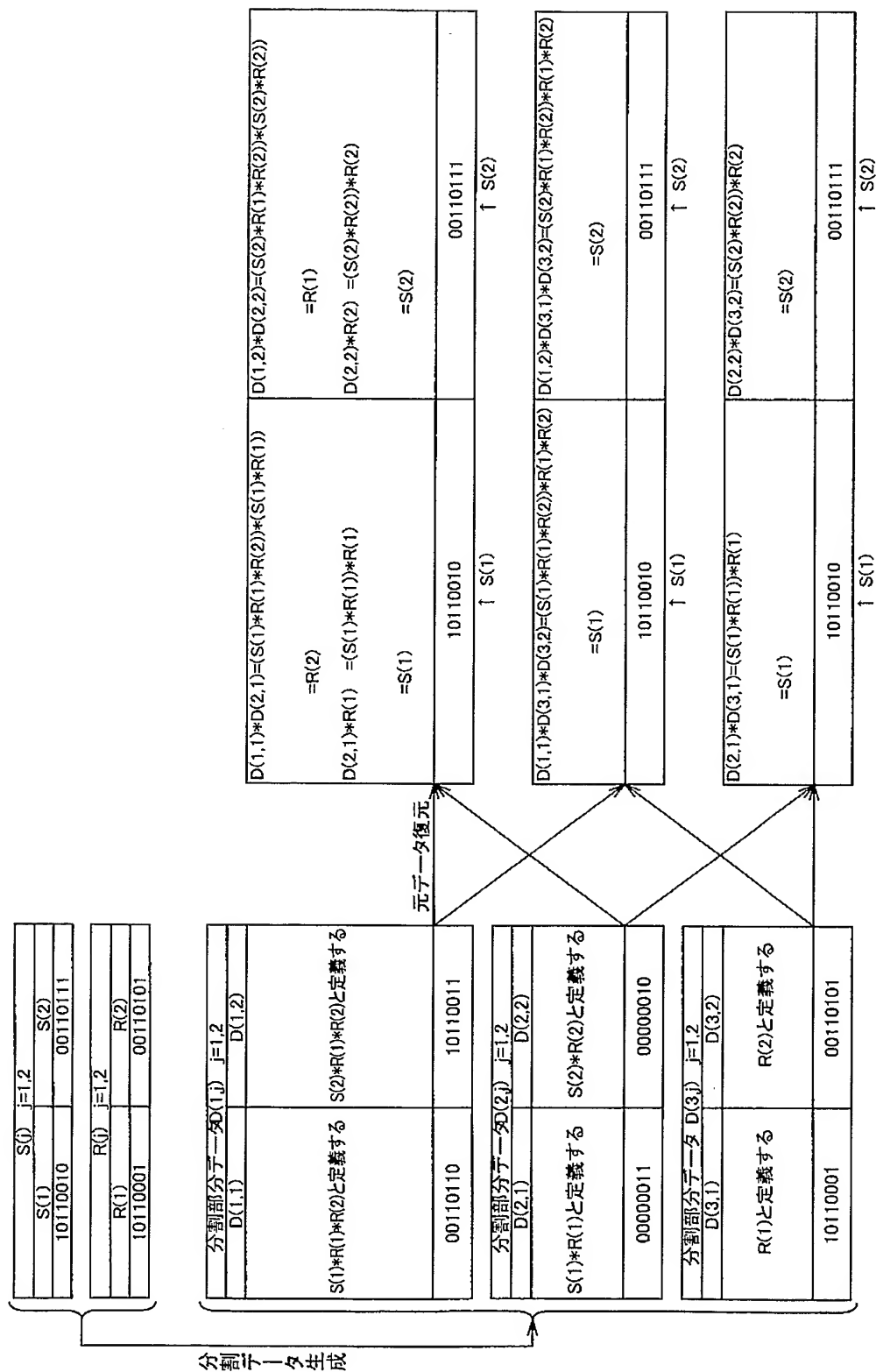
30 アクセス権管理システム

【図 6】





【図 7】

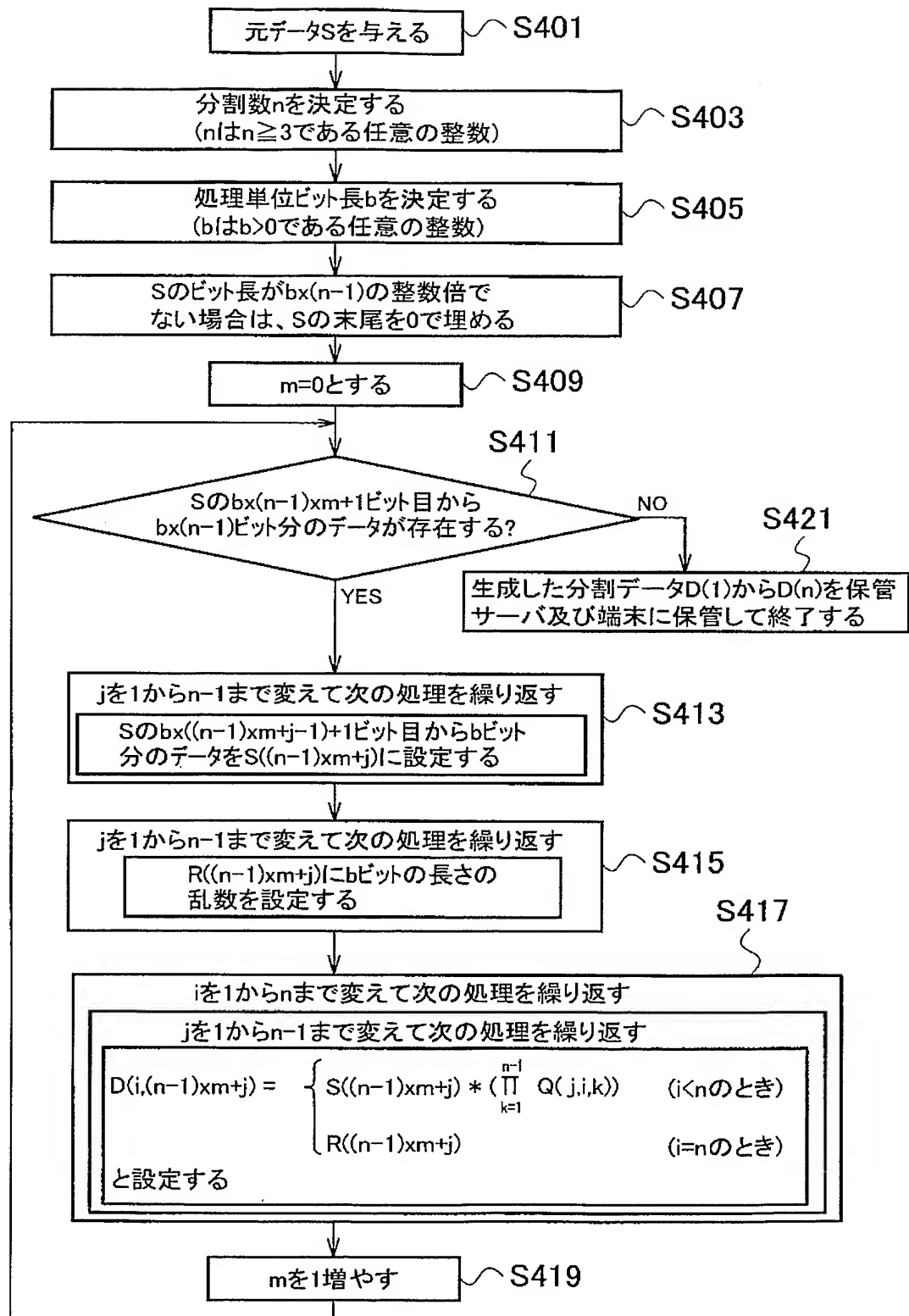


【図 8】

3分割 (n=3)
任意の2つの分割データから元データが復元可能。
(mはm>0の任意の整数) →元データSの末尾まで続く

jの値	1	2	...	j=2 × m+1	j+1	...
元データ S(j)	S(1)	S(2)	...	S(j)	S(j+1)	...
乱数 R(j)	R(1)	R(2)	...	R(j)	R(j+1)	...
分割データD(1,j)	S(1)*R(1)*R(2)	S(2)*R(1)*R(2)	...	S(j)*R(j)*R(j+1)	S(j+1)*R(j)*R(j+1)	...
分割データD(2,j)	S(1)*R(1)	S(2) *R(2)	...	S(j)*R(j)	S(j+1) *R(j+1)	...
分割データD(3,j)	R(1)	R(2)	...	R(j)	R(j+1)	...

【図 9】





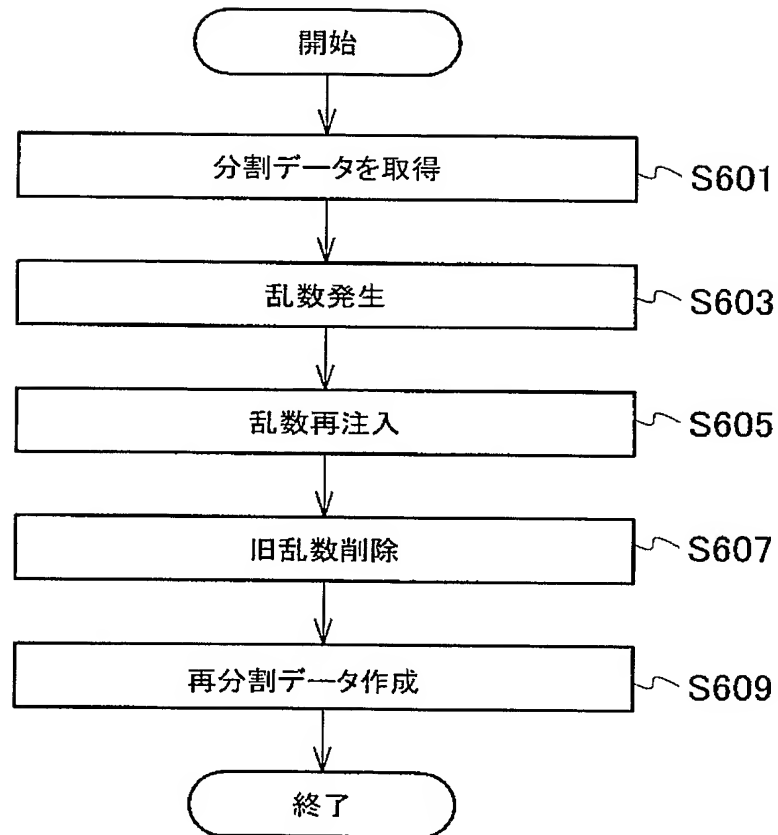
【図 10】

3分割 ($n=3$)

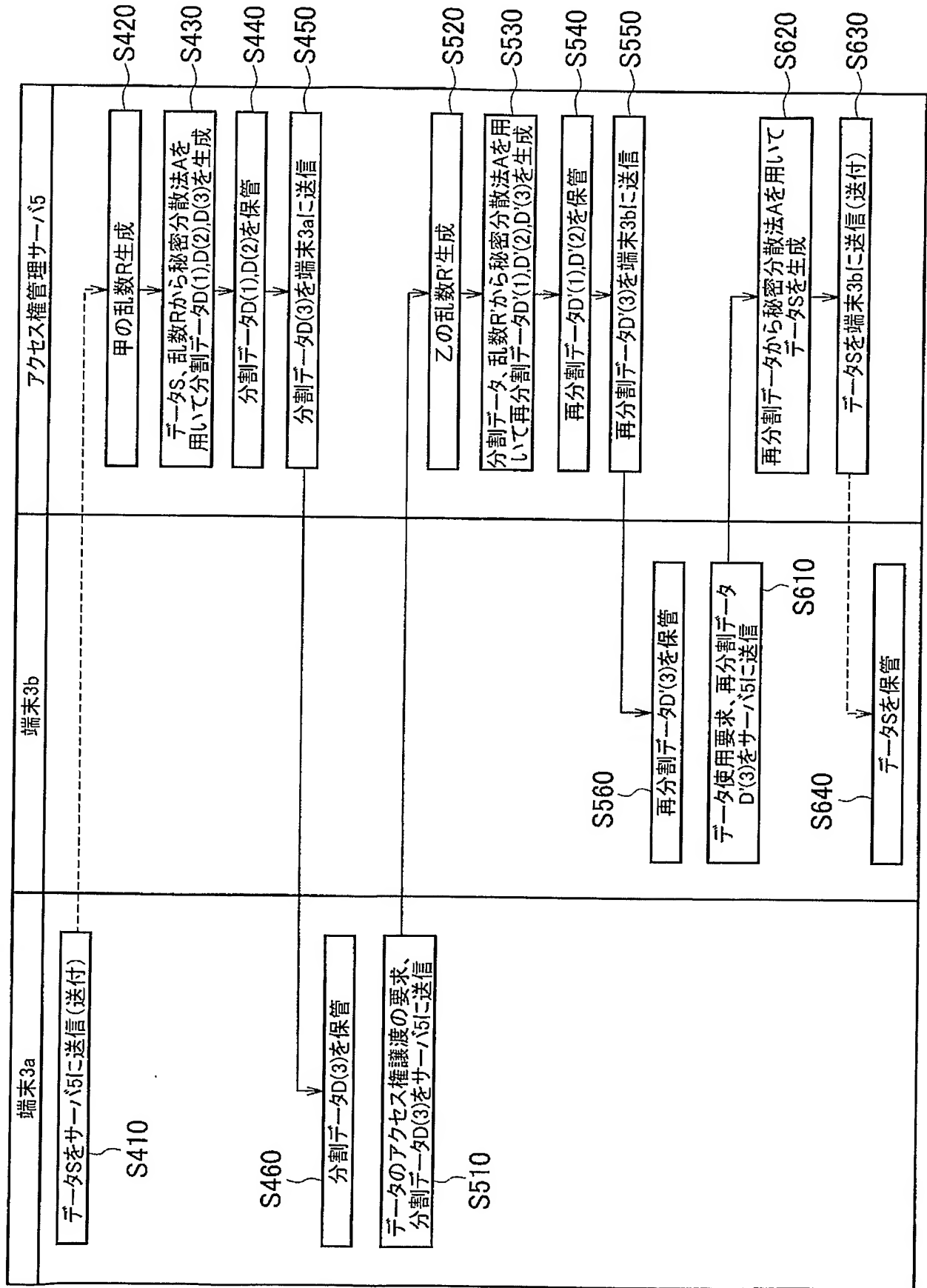
任意の2つの分割データから元データが復元可能。

		(mは $m>0$ の任意の整数)				→元データSの末尾まで続く	
jの値	1	2	...	$j=2 \times m+1$	$j+1$...
元データ S(j)	S(1)	S(2)	...	S(j)	S(j+1)		...
乱数 R(j)	R(1)	R(2)	...	R(j)	R(j+1)		...
分割データD(1,j)	$S(1)*R(1)*R(2)$	$S(2) * R(2)$...	$S(j)*R(j)*R(j+1)$	$S(j+1) * R(j+1)$...
分割データD(2,j)	$S(1)*R(1)$	$S(2)*R(1)*R(2)$...	$S(j)*R(j)$	$S(j+1)*R(j)*R(j+1)$...
分割データD(3,j)	R(1)	R(2)	...	R(j)	R(j+1)		...

【図 11】



【図 13】



【書類名】 要約書

【要約】

【課題】 暗号化によりアクセス制限されたデータのアクセス権限を他人に譲渡する場合であっても、データ復号化によるデータ漏洩の危険性を回避して、セキュリティを十分に確保することができる。

【解決手段】 端末 1 a において、甲の暗号鍵 R を用いてデータ S を暗号化した暗号化データ $A = S * R$ を生成し、保管するとともに、端末 1 b に暗号データ A を送信する。次に、端末 1 b においては、暗号データ A を受信すると、乙の暗号鍵 R' を用いて暗号データ A を暗号化し、暗号データ $A' = A * R'$ を生成し、端末 1 a に暗号データ A' を送信する。次に、端末 1 a においては、暗号データ A' を受信すると、さらに、甲の暗号鍵 R を用いて暗号データ A' を暗号化し、暗号データ $A'' = A' * R$ を生成し、端末 1 a から端末 1 b に暗号データ A'' を送信する。これにより、端末 1 b においては、受信した暗号データ A'' から乙の暗号鍵 R' を用いるとデータ S が復号化される。

【選択図】 図 2



特願 2 0 0 4 - 1 6 9 0 0 1

出 願 人 履 歴 情 報

識別番号

[3 9 9 0 3 5 7 6 6]

1. 変更新年月日

1 9 9 9 年 6 月 9 日

[変更理由]

新規登録

住 所

東京都千代田区内幸町一丁目 1 番 6 号

氏 名

エヌ・ティ・ティ・コミュニケーションズ株式会社